参考答案

（37）B

试题（38）

关于 Windows 操作系统中 DHCP 服务器的租约，下列说法中错误的是<u>（38）</u>。

（38）A．默认租约期是 8 天

B．客户端一直使用 DHCP 服务器分配给它的 IP 地址，直至整个租约期结束才开始联系更新租约

C．当租约期过了一半时，客户端将与提供 IP 地址的 DHCP 服务器联系更新租约

D．在当前租约期过去 87.5%时，如果客户端与提供 IP 地址的 DHCP 服务器联系不成功，则重新开始 IP 租用过程

试题（38）分析

通过在网络上安装和配置 DHCP 服务器，DHCP 的客户端可在每次启动并加入网络时动态地获得 IP 地址和相关配置参数。DHCP 服务器以地址租约的形式将该配置提供给发出请求的客户端。

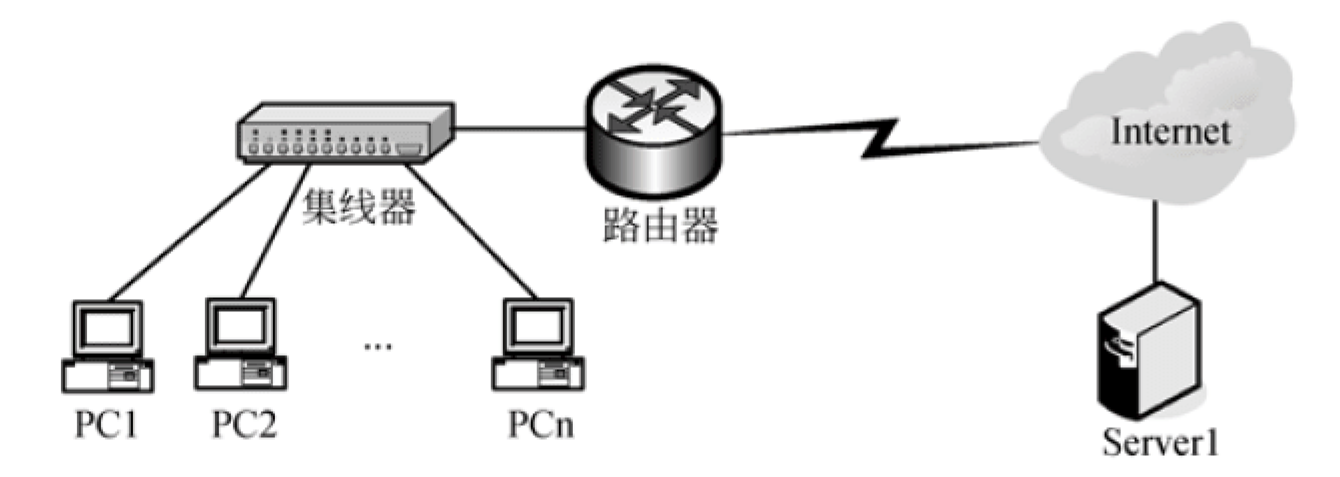
DHCP 的租约期限为 DHCP 服务器所分配的 IP 地址的有效期，租约定义了指派的 IP 地址可以使用的时间长度。默认情况下 DHCP 的租约期限为 8 天，当租约期过了一半时（按默认时间算是 4 天），客户端将和设置它的 TCP/IP 配置的 DHCP 服务器更新租约。当租期过了 87.5%时，如果客户端仍然无法与当初的 DHCP 服务器联系上，它将与其他 DHCP 服务器通信，如果网络上再没有任何 DHCP 服务器在运行时，该客户端必须停止使用该 IP 地址，并从发送一个 dhcpdiscover 数据包开始，再一次重复整个过程。

参考答案

（38）B

试题（39）

某网络结构如下图所示。除了 PC1 外其他 PC 都能访问服务器 Server1，造成 PC1 不能正常访问 Server1 的原因可能是<u>（39）</u>。



（39）A．PC1 设有多个 IP 地址　　　B．PC1 的 IP 地址设置错误

C．PC1 的子网掩码设置错误　　D．PC1 的默认网关设置错误

试题（39）分析

若PC1设有多个IP地址，某一时刻连接到Internet的只有一个，不是造成PC1不能访问服务器Server1的原因；图中各PC采用集线器而不是交换机进行连接，各PC不需要设置在同一网段，因此IP地址设置错误或子网掩码设置错误也不是造成PC1不能正常访问Server1的原因。若PC1的默认网关设置错误，则不能连接Internet。

默认网关对于有效地运行IP路由非常重要。在多数情况下，充当TCP/IP主机的默认网关的路由器（专用路由器或者连接两个或更多网段的计算机）维护大型网络中其他网络的信息以及访问这些网络的方法。

TCP/IP主机依赖默认网关来满足大多数与远程网段上的主机通信的需要。这样，单独主机就免去了需要维护单独远程IP网段的广泛而持续的信息更新的负担。只有充当默认网关的路由器才需要维护访问大型互联网络中的远程网段这个级别上的路由信息。

如果默认网关出现故障，则本地网段之外的通信可能会减弱。为了防止发生这种情况，可以使用“高级TCP/IP设置”对话框（在“网络连接”中）来为每一个连接指定多个默认网关。也可以使用route命令手动向路由表添加经常使用的主机或网络的路由。

参考答案

（39）D

试题（40）

为保障Web服务器的安全运行，对用户要进行身份验证。关于Windows Server 2003中的“集成Windows身份验证”，下列说法中错误的是<u>（40）</u>。

（40）A．在这种身份验证方式中，用户名和密码在发送前要经过加密处理，所以是一种安全的身份验证方案

B．这种身份验证方案结合了Windows NT质询/响应身份验证和Kerberos v5身份验证两种方式

C．如果用户系统在域控制器中安装了活动目录服务，而且浏览器支持Kerberos v5身份认证协议，则使用Kerberos v5身份验证

D．客户端通过代理服务器建立连接时，可采用集成Windows身份验证方案进行验证

试题（40）分析

在集成Windows身份验证方式中，用户名和密码在发送前要要经过加密处理，所以是一种安全的身份验证方案。这种身份验证方案结合了Windows NT质询/响应身份验证（NTLM）和Kerberos v5身份验证两种方式。Kerberos v5是Windows 2000分布式服务架构的重要功能，为了进行Kerberos v5身份验证，客户端和服务器都必须与密钥发行中心（KDC）建立可信任的连接。如果用户系统在域控制器中安装了Active Directory服务，而且浏览器支持Kerberos v5身份认证协议，则使用Kerberos v5身份验证，否则使用NTLM身份验证。

集成 Windows 身份验证的过程如下：

（1）在这种认证方式下，用户不必输入凭据，而是使用客户端上当前的 Windows 用户信息作为输入的凭据；

（2）如果最初的信息交换未能识别用户的合法身份，则浏览器将提示用户输入账号和密码，直到用户输入了有效的账号和密码，或者关闭了提示对话框。

集成 Windows 身份验证方案虽然比较安全，但是通过代理服务器建立连接时这个方案就行不通了。所以集成 Windows 身份验证最适合于 Intranet 环境，这样用户和 Web 服务器都在同一个域内，而且管理员可以保证每个用户浏览器都在 IE 2.0 版本以上，保证支持这种身份验证方案。

参考答案

（40）D

试题（41）、（42）

SNMPv1 使用__（41）__进行报文认证，这个协议是不安全的。SNMPv3 定义了__（42）__的安全模型，可以使用共享密钥进行报文认证。

（41）A．版本号（Version）　　B．协议标识（Protocol ID）
C．团体名（Community）　　D．制造商标识（Manufacturer ID）

（42）A．基于用户　　B．基于共享密钥
C．基于团体　　D．基于报文认证

试题（41）、（42）分析

SNMPv1 使用团体名进行报文认证，这个协议是不安全的。SNMPv3 定义了基于用户的安全模型（USM），可以使用共享密钥进行报文认证。

参考答案

（41）C　（42）A

试题（43）

若在 Windows“运行”窗口中输入__（43）__命令，则可运行 Microsoft 管理控制台。

（43）A．CMD　　B．MMC　　C．AUTOEXE　　D．TTY

试题（43）分析

运行 Microsoft 管理控制台，必须在 Windows“运行”窗口中输入“MMC”，MMC 是 Microsoft Management Console 的缩写。

参考答案

（43）A

试题（44）

在 Windows 操作系统中，如果要查找从本地出发，经过 3 个跳步，到达名字为 Enric 的目标主机的路径，则输入的命令是__（44）__。

（44）A．tracert Enric-h 3　　B．tracert -j 3 Enric

C．tracert -h 3 Enric D．tracert Enric -j 3

试题（44）分析

tracert 命令的用法如下：

```
C:\windows\> tracert [-d] [-h maximum _hops] [-j hop-list] [-w timeout]
<target _name>
```

其中，

-d 不将 IP 地址解析成主机名；

-h max-hops 指定了最大跟踪跳步数；

-j hop-list 指定了有限源路由；

-w timeout 指定了响应的超时时间，单位是毫秒。

参考答案

（44）C

试题（45）

能显示 TCP 和 UDP 连接信息的命令是__（45）__。

（45）A．netstat -s B．netstat -e C．netstat -r D．netstat -a

试题（45）分析

netstat 命令的用法如下：

```
C:\windows\> netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

其中，

-a 显示所有连接和处于监听状态的接口（服务器端的连接通常不显示）；

-c 显示所有以太网统计数据。这个选项可以跟-s 选项一起使用；

-n 用数字的形式显示地址和端口号；

-p proto 显示 proto 指定协议的连接，proto 的取值可以是 TCP 或 UDP，如果配合-s 选项则可以显示每个协议的统计数据，proto 的取值可以是 TCP、UDP 或 IP；

-r 显示路由表的内容；

-s 显示每个协议的统计数据，默认显示 TCP、UDP 和 IP 的统计数据，利用-p 选项可以指定只显示其中一部分；

interval 每隔 inteval 秒重复显示指定的统计数据，按 CTRL+C 组合键可终止显示，如果不指定 interval，netstat 会将当前的信息显示一次。

参考答案

（45）D

试题（46）

设有两个子网 202.118.133.0/24 和 202.118.130.0/24，如果进行路由汇聚，得到的网络地址是__（46）__。

（46）A．202.118.128.0/21　　B．202.118.128.0/22

C．202.118.130.0/22　　D．202.118.132.0/20

试题（46）分析

网络 202.118.133.0/24 的二进制表示为：　**11001010 01110110 10000**101 00000000

网络 202.118.130.0/24 的二进制表示为：　**11001010 01110110 10000**010 00000000

两者的共同部分是（见黑体部分）：　**11001010 01110110 10000**000 00000000

所以经路由汇聚后得到的超网为 202.118.128.0/21。

参考答案

（46）A

试题（47）

路由器收到一个数据包，其目标地址为 195.26.17.4，该地址属于 （47） 子网。

（47）A．195.26.0.0/21　　B．195.26.16.0/20

C．195.26.8.0/22　　D．195.26.20.0/22

试题（47）分析

网络 195.26.0.0/21 的二进制表示为：　**11000011 00011010 00000**000 00000000

网络 195.26.16.0/20 的二进制表示为：　**11000011 00011010 0001**0000 00000000

网络 195.26.8.0/22 的二进制表示为：　**11000011 00011010 000010**00 00000000

网络 195.26.20.0/22 的二进制表示为：　**11000011 00011010 000101**00 00000000

地址 195.26.17.4 二进制表示为：　**11000011 00011010 0001**0001 00000100

可以看出，选项 B 中的网络与地址 195.26.17.4 满足最长匹配规则，所以地址 195.26.17.4 所属的子网是 195.26.16.0/20。

参考答案

（47）B

试题（48）

主机地址 172.16.2.160 属于下面哪一个子网？ （48）

（48）A．172.16.2.64/26　　B．172.16.2.96/26

C．172.16.2.128/26　　D．172.16.2.192/26

试题（48）分析

网络 172.16.2.64/26 的二进制表示为：　**10101100 00010000 00000010 01**000000

网络 172.16.2.96/26 的二进制表示为：　**10101100 00010000 00000010 01**100000

网络 172.16.2.128/26 的二进制表示为：　**10101100 00010000 00000010 10**000000

网络 172.16.2.192/26 的二进制表示为：　**10101100 00010000 00000010 11**000000

地址 192.15.2.160 二进制表示为：　**10101100 00010000 00000010 10**100000

可以看出，只有选项 C 中的网络 172.16.2.128/26 与地址 172.16.2.160 前 26 位相匹配。

参考答案

（48）C

试题（49）

如果用户网络需要划分成 5 个子网，每个子网最多 20 台主机，则适用的子网掩码是 __（49）__。

（49）A．255.255.255.192　　B．255.255.255.240

C．255.255.255.224　　D．255.255.255.248

试题（49）分析

由于要划分成 5 个子网，需要 3 位来表示子网号；每个子网最多 20 台主机，需要 5 位来表示主机地址，网络地址部分为 24 位，所以地址掩码为 255.255.255.224，如下图所示。

网络号	子网号	主机号
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 1	0 0 0 0 0

参考答案

（49）C

试题（50）

CIDR 技术的作用是 __（50）__。

（50）A．把小的网络汇聚成大的超网　　B．把大的网络划分成小的子网

C．解决地址资源不足的问题　　D．由多个主机共享同一个网络地址

试题（50）分析

CIDR 技术的作用是把小的网络汇聚成大的超网，VLSM 技术的作用是把大的网络划分成小的子网。

参考答案

（50）A

试题（51）

路由器命令 Router>sh int 的作用是 __（51）__。

（51）A．检查端口配置参数和统计数据　　B．进入特权模式

C．检查是否建立连接　　D．检查配置的协议

试题（51）分析

路由器命令 Router>sh int 的作用是检查端口配置参数和统计数据，全写为

```
Router>show interface
```

参考答案

（51）A

试题（52）

下面列出了路由器的各种命令状态，可以配置路由器全局参数的是 __（52）__。

（52）A．router>　　B．router#　　C．router(config)#　　D．router(config-if)#

试题（52）分析

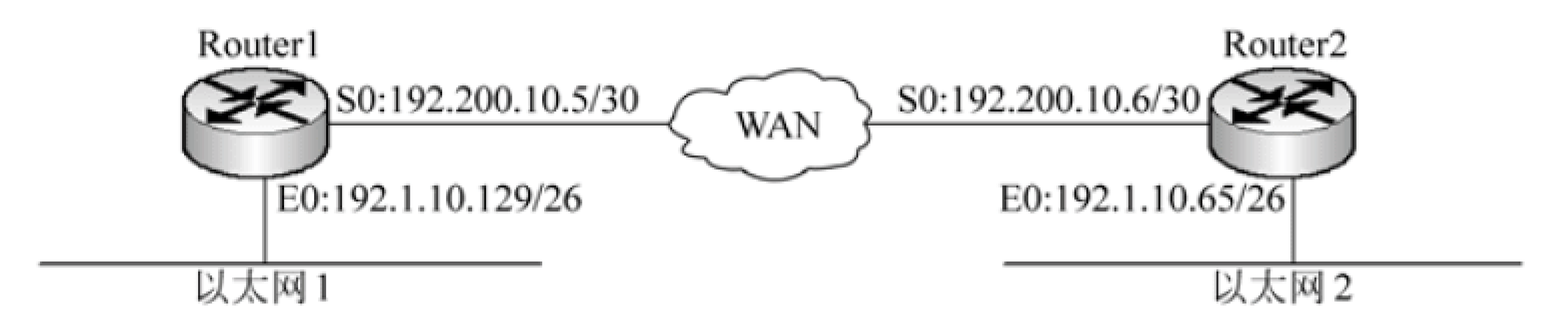
router>	用户执行模式提示符
router>enable	输入特权模式命令
router#	特权模式提示符
router#config term	进入配置模式命令
router(config)#	全局配置模式提示符
router(config)#int f0/1	进入接口配置模式
router(config-if)#	接口配置模式提示符

参考答案

（52）C

试题（53）

网络配置如下图所示，为路由器 Router1 配置访问以太网 2 的命令是__（53）__。



（53）A．ip　route　192.1.10.60　255.255.255.192　192.200.10.6
　　　B．ip　route　192.1.10.65　255.255.255.26　192.200.10.6
　　　C．ip　route　192.1.10.64　255.255.255.26　192.200.10.65
　　　D．ip　route　192.1.10.64　255.255.255.192　192.200.10.6

试题（53）分析

为路由器 Router1 配置访问以太网 2 的命令如下：

```
ip route 192.1.10.64 255.255.255.192 192.200.10.6
```

参考答案

（53）D

试题（54）

可以采用静态或动态方式来划分 VLAN，下面属于静态划分的方法是__（54）__。

（54）A．按端口划分　　B．按 MAC 地址划分
　　　C．按协议类型划分　　D．按逻辑地址划分

试题（54）分析

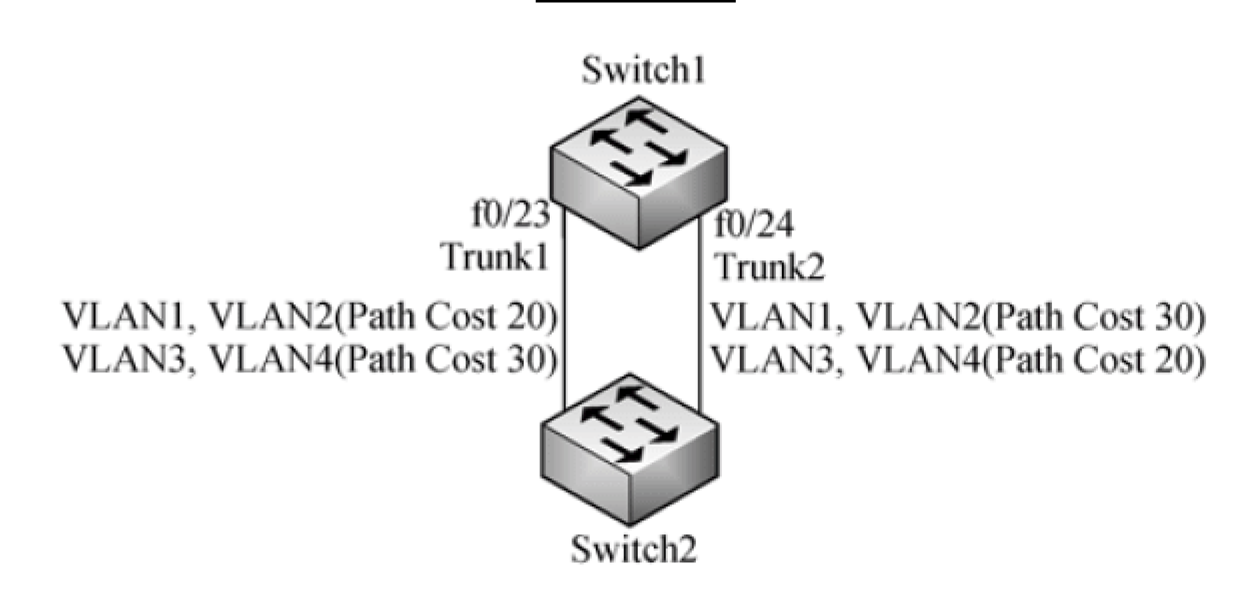
按端口划分属于静态划分的方法，这时终端就被绑定在端口上了。如果按 MAC 地址或协议类型划分，在终端可以移动到别的端口上去。

参考答案

（54）A

试题（55）、（56）

如果两个交换机之间设置多条 Trunk，则需要用不同的端口权值或路径费用来进行负载均衡。默认情况下，端口的权值是 （55） 。在如下图所示的配置下， （56） 。



（55）A．64 B．128 C．256 D．1024

（56）A．VLAN1 的数据通过 Trunk1，VLAN2 的数据通过 Trunk2

B．VLAN1 的数据通过 Trunk1，VLAN3 的数据通过 Trunk2

C．VLAN2 的数据通过 Trunk2，VLAN4 的数据通过 Trunk1

D．VLAN2 的数据通过 Trunk2，VLAN3 的数据通过 Trunk1

试题（55）、（56）分析

默认情况下，端口的权值是 128。如果端口权值相同，则选择路径费用小的链路进行传输。在图中所示的配置下，VLAN1 和 VLAN2 在 Trunk1 上的费用小，VLAN3 和 VLAN4 在 Trunk2 上的费用小。

参考答案

（55）B （56）B

试题（57）

在以太网中，最大传输单元（MTU）是 （57） 个字节。

（57）A．46 B．64 C．1500 D．1518

试题（57）分析

在以太网中，最大传输单元（MTU）是 1500 个字节，最大帧长是 1518 个字节。

参考答案

（57）C

试题（58）

在下面关于以太网与令牌环网性能的比较中，正确的是 （58） 。

（58）A．在重负载时，以太网比令牌环网的响应速度快

B．在轻负载时，令牌环网比以太网的利用率高

C．在重负载时，令牌环网比以太网的利用率高

D．在轻负载时，以太网比令牌环网的响应速度慢

试题（58）分析

在重负载时，令牌环网比以太网的利用率高，令牌每经过一站，都有数据帧发送，网络充分忙碌。

参考答案

（58）C

试题（59）

确定网络的层次结构及各层采用的协议是网络设计中＿（59）＿阶段的主要任务。

（59）A．网络需求分析　　B．网络体系结构设计

C．网络设备选型　　D．网络安全性设计

试题（59）分析

网络方案的设计主要包括网络需求分析，网络体系结构设计，网络安全性设计设备选型等设计规划过程。

在网络需求分析阶段主要完成：① 了解企业用户的现状；② 弄清用户的目的；③ 掌握资金投入的额度；④ 了解企业用户环境；⑤ 确定企业用户的数据流管理架构。在了解了用户的网络需求之后，要根据标准化、规范化、先进性、扩充性、可靠性、安全性、可管理性、可维护性、实用性、灵活性和经济性等确定建网原则。

在确定好建网原则之后，可以开始网络总体设计工作，总体规划主要包括网络体系结构设计阶段、网络安全性设计阶段和网络设备选型阶段。在网络体系结构设计阶段的主要任务是确定网络的层次结构及各层采用的协议，在网络安全性设计阶段的主要任务是完成可靠性与容错设计和网络安全体系的设计，在网络设备选型阶段的主要任务是根据体系结构、安全性要求和结合经济可行性等确定网络设备的选型。

参考答案

（59）B

试题（60）

在层次化园区网络设计中，＿（60）＿是接入层的功能。

（60）A．高速数据传输　　B．VLAN 路由

C．广播域的定义　　D．MAC 地址过滤

试题（60）分析

层次化网络设计设计在互联网组件的通信中引入了三个关键层的概念，这三个层次分别是：核心层（Core Layer）、汇聚层（Distribution Layer）和接入层（Access Layer）。

核心层为网络提供了骨干组件或高速交换组件，高速数据传输是核心层的目标。

汇聚层是核心层和终端用户接入层的分界面，汇聚层完成网络访问策略控制、广播域的定义、VLAN 间路由、数据包处理、过滤、寻址及其他数据处理的任务。

接入层向本地网段提供用户接入，主要提供网络分段、广播能力、多播能力、介质访问的安全性、MAC 地址过滤和路由器发现等任务。

参考答案

（60）D

试题（61）

园区网络设计中，如果网络需求对 QoS 要求很高，应考虑采用__（61）__网络。

（61）A．ATM　　B．千兆以太　　C．FDDI　　D．ISDN

试题（61）分析

目前的 Internet 仅提供尽力而为（best-effort service）的传输服务，业务量尽快传输，没有明确的时间和可靠性保障。随着网络多媒体技术的飞速发展，Internet 上的多媒体应用层出不穷，如 IP 电话、视频会议、视频点播（VOD）、远程教育等多媒体实时业务以及电子商务在 Internet 上传输等。Internet 已逐步从单一的数据传输网向数据、语音、图像等多媒体信息的综合传输网演化。各种应用对服务质量的需求在迅速增长，这些不同的应用需要有不同的 QoS（Quality of Service）要求，QoS 通常用带宽、时延、时延抖动和分组丢失率来衡量。QoS 的关键指标包括可用性、吞吐量、时延、时延变化（包括抖动和漂移）和丢失。

ATM 的最大的优势在于可以有效地实现 QoS，传统的 IP 技术正在逐步与 ATM 技术相结合，目前 IP 与 ATM 结合技术有 ATM Forum 定义的 LANE；IETF 定义的 CIPOA；ATM Forum 定义的 MPOA；IETF 制定的多协议标签交换（Multiprotocol label switching，MPLS）。

参考答案

（61）（A）

试题（62）

在 IPv4 中，组播地址是__（62）__地址。

（62）A．A 类　　B．B 类　　C．C 类　　D．D 类

试题（62）分析

IP 组播（也称多址广播或多播）技术，是一种允许一台或多台主机（组播源）发送单一数据包到多台主机（一次的、同时的）的 TCP/IP 网络技术。组播作为一点对多点的通信，是节省网络带宽的有效方法之一。在网络音频/视频广播的应用中，当需要将一个结点的信号传送到多个结点时，无论是采用重复点对点通信方式，还是采用广播方式，都会严重浪费网络带宽，只有组播才是最好的选择。组播能使一个或多个组播源只把数据包发送给特定的组播组，而只有加入该组播组的主机才能接收到数据包。目前，IP 组播技术被广泛应用在网络音频/视频广播、AOD/VOD、网络视频会议、多媒体远程教育、push 技术（如股票行情等）和虚拟现实游戏等方面。

IP 组播通信必须依赖于 IP 组播地址，在 IPv4 中它是一个 D 类 IP 地址，范围为

224.0.0.0～239.255.255.255，并被划分为局部链接组播地址、预留组播地址和管理权限组播地址三类。其中，局部链接组播地址范围为 224.0.0.0～224.0.0.255，这是为路由协议和其他用途保留的地址，路由器并不转发属于此范围的 IP 包；预留组播地址范围为 224.0.1.0～238.255.255.255，可用于全球范围（如 Internet）或网络协议；管理权限组播地址范围为 239.0.0.0～239.255.255.255，可供组织内部使用，类似于私有 IP 地址，不能用于 Internet，可限制组播范围。

参考答案

（62）D

试题（63）

以下关于 Samba 的描述中，不正确的是＿（63）＿。

（63）A．Samba 采用 SMB 协议
B．Samba 支持 WINS 名字解析
C．Samba 向 Linux 客户端提供文件和打印机共享服务
D．Samba 不支持 Windows 的域用户管理

试题（63）分析

Samba 采用 SMB 协议，支持 WINS 名字解析，并且向 Linux 客户端提供文件和打印机共享服务，还支持 Windows 的域用户管理。

参考答案

（63）D

试题（64）

ADSL 采用的两种接入方式是＿（64）＿。

（64）A．虚拟拨号接入和专线接入　　B．虚拟拨号接入和虚电路接入
C．虚电路接入和专线接入　　D．拨号虚电路接入和专线接入

试题（64）分析

ADSL 采用的两种接入方式是虚拟拨号接入和专线接入。虚拟拨号就是和普通 56K MODEM 拨号一样，通过 PPPoE 协议进行账号验证、IP 地址分配等过程建立连接，是面向家庭用户的接入方式。ADSL 专线接入是在用户安装好 ADSL MODEM 后，在 PC 中配置 IP 地址和子网掩码、默认网关等参数，开机后用户端和局端自动建立起一条链路。所以专线接入方式是有固定 IP 地址的接入方式，费用较高，多在大型网吧中使用。

参考答案

（64）A

试题（65）

在 Web Services 中，客户与服务之间的标准通信协议是＿（65）＿。

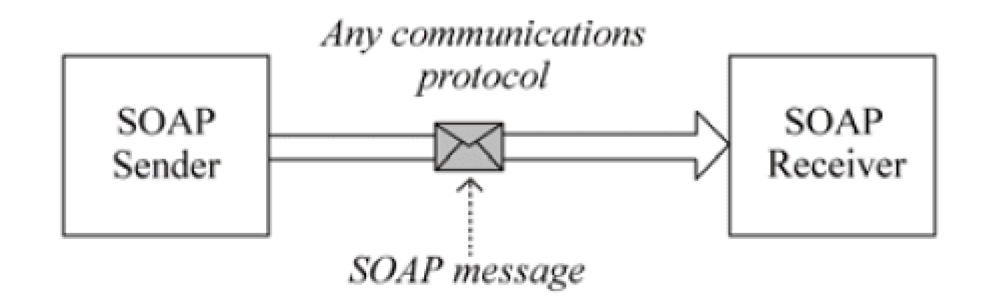
（65）A．简单对象访问协议　　B．超文本传输协议
C．统一注册与发现协议　　D．远程对象访问协议

试题（65）分析

在 Web Services 中，客户与服务之间的标准通信协议是简单对象访问协议（SOAP）。

SOAP 是一种轻量级协议，用于在分散型、分布式环境中交换结构化信息。 SOAP 利用 XML 技术定义一种可扩展的消息处理框架，它提供了一种可通过多种底层协议进行交换的消息结构。这种框架的设计思想是要独立于任何一种特定的编程模型和其他特定实现的语义。

SOAP 定义了一种方法以便将 XML 消息从 A 点传送到 B 点（参见下图）。为此，它提供了一种基于 XML 且具有以下特性的消息处理框架：① 可扩展；② 可通过多种底层网络协议使用；③ 独立于编程模型。



参考答案

（65）A

试题（66）～（70）

NAC's（Network Access Control） role is to restrict network access to only compliant endpoints and __(66)__ users. However, NAC is not a complete LAN __(67)__ solution; additional proactive and __(68)__ security measures must be implemented. Nevis is the first and only comprehensive LAN security solution that combines deep security processing of every packet at 10Gbps, ensuring a high level of security plus application availability and performance. Nevis integrates NAC as the first line of LAN security __(69)__. In addition to NAC, enterprises need to implement role-based network access control as well as critical proactive security measures — real-time, multilevel __(70)__ inspection and microsecond threat containment.

（66）A. automated　B. distinguished　C. authenticated　D. destructed
（67）A. crisis　B. security　C. favorable　D. excellent
（68）A. constructive　B. reductive　C. reactive　D. productive
（69）A. defense　B. intrusion　C. inbreak　D. protection
（70）A. port　B. connection　C. threat　D. insurance

参考译文

网络访问控制（NAC）的作用是限制对网络的访问，只允许注册的终端和认证的用户访问网络。然而 NAC 不是一个完整的 LAN 安全解决方案，另外还要实现主动的和被动的安全手段。Nevis 是第一个也是仅有的全面的 LAN 安全解决方案，它以 10Gbps 的

速率对每一个分组进行深度的安全处理，在提供高级别安全的同时能保证网络应用的可利用性和适当的性能。Nevis 集成了 NAC 作为 LAN 的第一道安全防线。此外，企业还需要实现基于角色的网络访问控制以及起关键作用的主动安全测试——实时的多级安全威胁检测和微秒级的安全威胁堵截。集中的安全策略配置、管理和报告使其能够迅速地对问题进行分析，对用户的活动进行跟踪，这些都是实时可见的，也是历史可查的。

参考答案

（66）C　（67）B　（68）C　（69）A　（70）C

试题（71）～（75）

Virtualization is an approach to IT that pools and shares __(71)__ so that utilization is optimized and supplies automatically meet demand. Traditional IT environments are often silos, where both technology and human __(72)__ are aligned around an application or business function. With a virtualized __(73)__ , people, processes, and technology are focused on meeting service levels, __(74)__ is allocated dynamically, resources are optimized, and the entire infrastructure is simplified and flexible. We offer a broad spectrum of virtualization __(75)__ that allows customers to choose the most appropriate path and optimization focus for their IT infrastructure resources.

（71）A．advantages　B．resources　C．benefits　D．precedents
（72）A．profits　B．costs　C．resources　D．powers
（73）A．system　B．infrastructure　C．hardware　D．link
（74）A．content　B．position　C．power　D．capacity
（75）A．solutions　B．networks　C．interfaces　D．connections

参考译文

虚拟化是 IT 行业缓存和共享资源的一种方法，通过这种方法可以更好地利用资源，并且自动提供资源以满足需求。传统的 IT 环境通常是一个竖井，技术和人力资源都是围绕应用或商业功能来安排的。利用虚拟化的架构，人员、过程和技术都集中于满足服务的程度，生产量被动态地分配，资源得到优化，而且整个架构得以简化，变得很灵活。我们提供了广泛的虚拟化解决方案，允许客户为他们的 IT 资源的基础架构选择最适用的路线和优化的重点。

参考答案

（71）B　（72）C　（73）B　（74）D　（75）A

第 10 章　2006 下半年网络工程师下午试题分析与解答

试题一（15 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某学校计划建立校园网，拓扑结构如图 1-1 所示。该校园网分为核心、汇聚和接入三层，由交换模块、广域网接入模块、远程访问模块和服务器群四大部分构成。

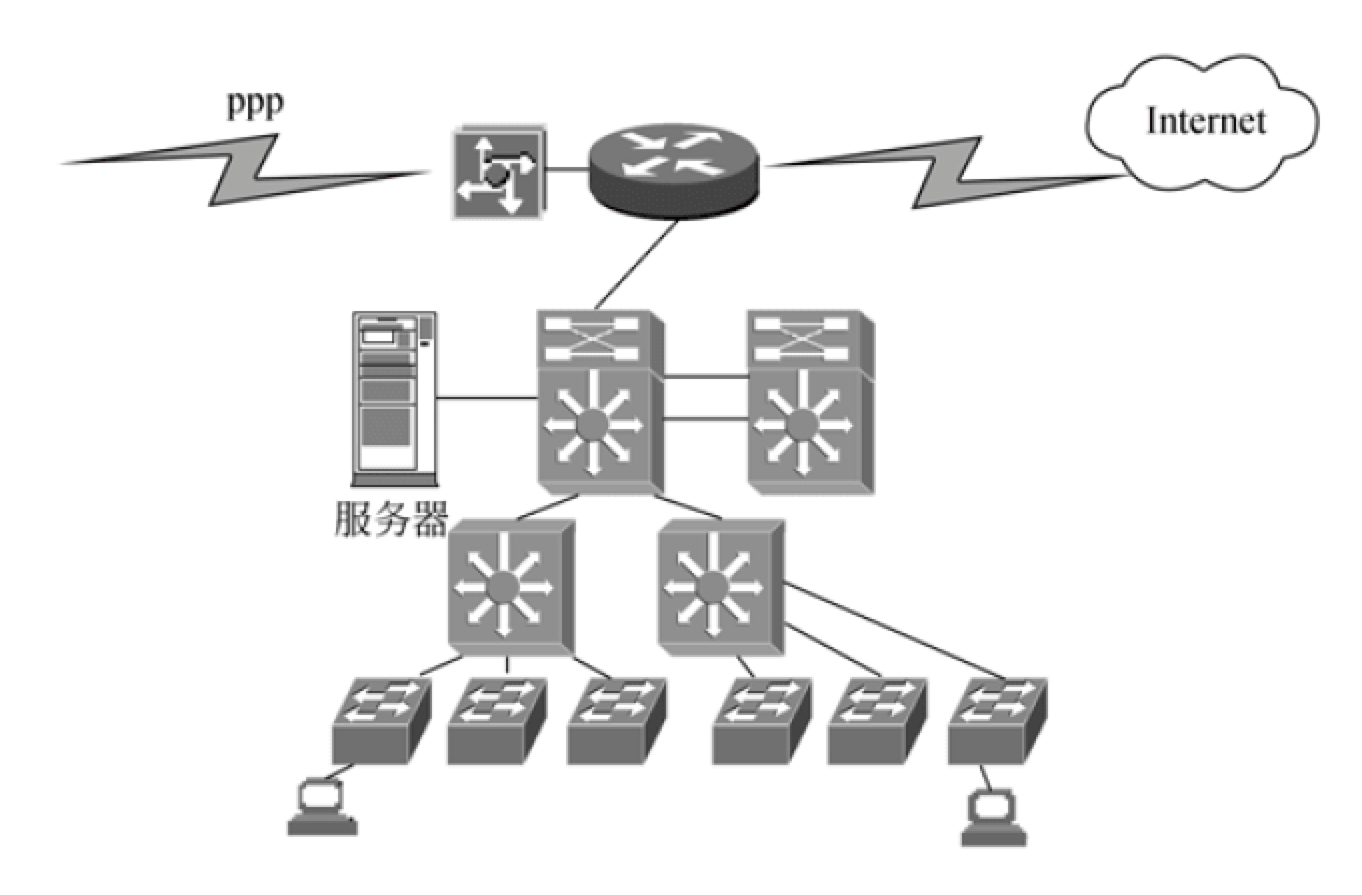


图 1-1

【问题 1】

在校园网设计过程中，划分了很多 VLAN，采用了 VTP 来简化管理。将（1）～（5）处空缺信息填写在答题纸对应的解答栏内。

1．VTP 信息只能在＿（1）＿端口上传播。

2．运行 VTP 的交换机可以工作在三种模式：＿（2）＿、＿（3）＿、＿（4）＿。

3．共享相同 VLAN 数据库的交换机构成一个＿（5）＿。

【问题 2】

该校园网采用了异步拨号进行远程访问，异步封装协议采用了 PPP 协议。将（6）～（9）处空缺信息填写在答题纸对应的解答栏内。

1．异步拨号连接属于远程访问中的电路交换服务，远程访问中另外两种可选的服务类型是：＿（6）＿和＿（7）＿。

2．PPP 提供了两种可选的身份认证方法，它们分别是＿（8）＿和＿（9）＿。

【问题 3】

该校园网内交换机数量较多，交换机间链路复杂，为了防止出现环路，需要在各交换机上运行__（10）__。

【问题 4】

该校园网在安全设计上采用分层控制方案，将整个网络分为外部网络传输控制层、内外网间访问控制层、内部网络访问控制层、操作系统及应用软件层和数据存储层，对各层的安全采取不同的技术措施。从备选答案中选择信息，将（11）～（14）处空缺信息填写在答题纸对应的解答栏内。

安全技术	对应层次
（11）	外部网络传输控制层
（12）	内外网间访问控制层
（13）	内部网络访问控制层
（14）	数据存储层

（11）～（14）处备选答案：

A．IP 地址绑定　　B．数据库安全扫描

C．虚拟专用网（VPN）技术　　D．防火墙

试题一分析

【问题 1】

本问题考查的是 VTP 的基本概念

在 VLAN 间需要通信的时候，可以利用 VLAN 间路由技术来实现。当网络管理人员需要管理的交换机数量众多时，可以使用 VLAN 中继协议（Vlan Trunking Protocol，VTP）简化管理，它只需要在一台交换机上定义所有 VLAN，然后通过 VTP 协议将 VLAN 定义传播到本管理域中的所有交换机上。这样，大大减轻了网络管理人员的工作负担和工作强度。

VTP（VLAN Trunk Protocol，VLAN 干道协议）的功能与 GVRP 相似，也是用来使 VLAN 配置信息在交换网内其他交换机上进行动态注册的一种二层协议。在一台 VTP Server 上配置一个新的 VLAN 信息，则该信息将自动传播到本域内的所有交换机，从而减少在多台设备上配置同一信息的工作量，并且方便了管理。VTP 信息只能在 Trunk 端口上传播。

任何一台运行 VTP 的交换机可以工作在以下三种模式：VTP Server、VTP Client 及 VTP Transparent。其中：

（1）VTP Server 维护该 VTP 域中所有 VLAN 信息列表，可以增加、删除或修改 VLAN；

（2）VTP Client 也维护该 VTP 域中所有 VLAN 信息列表，但不能增加、删除或修改

VLAN，任何变化的信息必须从 VTP Server 发布的通告报文中接收；

（3）VTP Transparent 不参与 VTP 工作，它虽然忽略所有接收到的 VTP 信息，但能够将接收到的 VTP 报文转发出去，它只拥有本设备上的 VLAN 信息；

交换 VTP 更新信息的所有交换机必须配置为相同的管理域。如果所有的交换机都以中继线相连，那么只要在核心交换机上设置一个管理域，网络上所有的交换机都将加入该域，这样管理域里所有的交换机就能够了解彼此的 VLAN 列表。

【问题 2】

本问题考查的是远程访问和异步拨号连接的知识。

远程访问是园区网络必须提供的服务之一。它可以为家庭办公用户和出差在外的员工提供移动接入服务。远程访问有三种可选的服务类型：专线连接、电路交换和包交换。不同的广域网连接类型提供的服务质量不同，花费也不相同。

异步拨号连接属于电路交换类型的广域网连接，它是在传统公共交换电话网（Public Switched Telephone Network，PSTN）上提供服务的。传统 PSTN 提供的服务也被称为简易老式电话业务（Plan Old Telephone System，POTS）。因为目前存在着大量安装好的电话线，所以这样的环境是最容易满足的。因此，异步拨号连接也就成为最为方便和普遍的远程访问类型。

广域网连接可以采用不同类型的封装协议，如 HDLC、PPP 等。其中，PPP 除了提供身份认证功能外，还可以提供其他很多可选项配置，包括链路压缩、多链路捆绑和回叫等，因此更具优势。PPP 提供了两种可选的身份认证方法：口令验证协议 PAP（Password Authentication Protocol，PAP）和质询握手协议（Challenge Handshake Authentication Protocol，CHAP）。

PAP 是一个简单的、实用的身份验证协议。PAP 认证进程只在双方的通信链路建立初期进行。如果认证成功，在通信过程中不再进行认证；如果认证失败，则直接释放链路。

CHAP 认证比 PAP 认证更安全，因为 CHAP 不在线路上发送明文密码，而是发送经过摘要算法加工过的随机序列，也被称为“挑战字符串”。同时，身份认证可以随时进行，包括在双方正常通信过程中。因此，非法用户就算截获并成功破解了一次密码，此密码也将在一段时间内失效。CHAP 对端系统要求很高，因为需要多次进行身份质询、响应，要耗费较多的 CPU 资源，因此只用在对安全要求很高的场合。PAP 虽然有着用户名和密码是明文发送的弱点，但是认证只在链路建立初期进行，因此节省了宝贵的链路带宽。

【问题 3】

本问题考查的是生成树协议方面的知识。

生成树协议（Spanning Tree）定义在 IEEE 802.1D 中，是一种链路管理协议，它为网络提供路径冗余的同时防止产生环路。为使以太网更好地工作，两个工作站之间只能有一条活动路径。

STP 允许网桥之间相互通信以发现网络物理环路。该协议定义了一种算法，网桥能够使用它创建无环路（loop-free）的逻辑拓扑结构。换句话说，STP 创建了一个由无环路树叶和树枝构成的树结构，跨越了整个第二层网络。

生成树协议操作对终端站透明，也就是说，终端站并不知道它们自己是否连接在单个局域网段或多网段中。当有两个网桥同时连接相同的计算机网段时，生成树协议可以允许两网桥之间相互交换信息，这样只需要其中一个网桥来处理两台计算机之间传输的信息。

【问题 4】

在网络安全方面，可以采用分层控制方案，将整个网络分为外部网络传输控制层、内外网间访问控制层、内部网络访问控制层、操作系统及应用软件层和数据存储层，进而对各层的安全采取不同的技术措施。

1．外部网络传输控制层

外部网络是指局域网路由器和防火墙之外的公用网。当前网络技术发展迅速，因特网四通八达，网上黑客手段多种多样，为了保证安全，可以从以下方面采取措施：虚拟专网（VPN）技术；身份认证技术；加密技术；物理隔离等。

2．内外网间访问控制层

在内部局域网和外部网络之间，可以采用以下技术来对外部和内部网络间的访问进行控制：防火墙；防毒网关；网络地址转换技术；代理服务及路由器；入侵检测等。

3．内部网访问控制层

在局域网内部，非法用户的登录和对数据的非法修改更加不易查出。当用户安全意识差、口令选择或保存不慎、账号转借和共享都会对网络安全造成极大的威胁，从内部网访问控制层进行安全防护，可采取以下措施：用户的身份认证；权限控制；加密技术；客户端安全防护等。

4．数据存储层

数据存储在服务器或加密终端上，数据存储的安全性是系统安全性的重要组成部分。对数据的安全保护措施可以采用以下几种方式：使用较安全的数据库系统；加密技术；数据库安全扫描；存储介质的安全等。

参考答案

【问题 1】

（1）Trunk

（2）VTP Server 或服务器模式

（3）VTP Client 或客户端模式

（4）VTP Transparent 或透明模式

（2），（3），（4）处答案次序任意

（5）VTP 管理域

【问题 2】

（6）专线连接

（7）分组交换

（6），（7）处答案可以互换

（8）口令认证协议（Password Authentication Protocol，PAP）

（9）质询握手认证协议（Challenge Handshake Authentication Protocol，CHAP）

（8），（9）处答案可以互换

【问题 3】

（10）生成树协议（Spanning Tree Protocol，STP）

【问题 4】

（11）C 或虚拟专用网（VPN）技术

（12）D 或防火墙

（13）A 或 IP 地址绑定

（14）B 或数据库安全扫描

试题二（15 分）

阅读以下关于 Linux 网关安装和配置过程的说明，回答问题 1 至问题 5。

【说明】

当局域网中存在大量计算机时，根据业务的不同，可以将网络分成几个相对独立的子网。图 2-1 是某公司子网划分的示意图，整个网络被均分为销售部和技术部两个子网，子网之间通过一台安装了 Linux 操作系统的双网卡计算机联通。

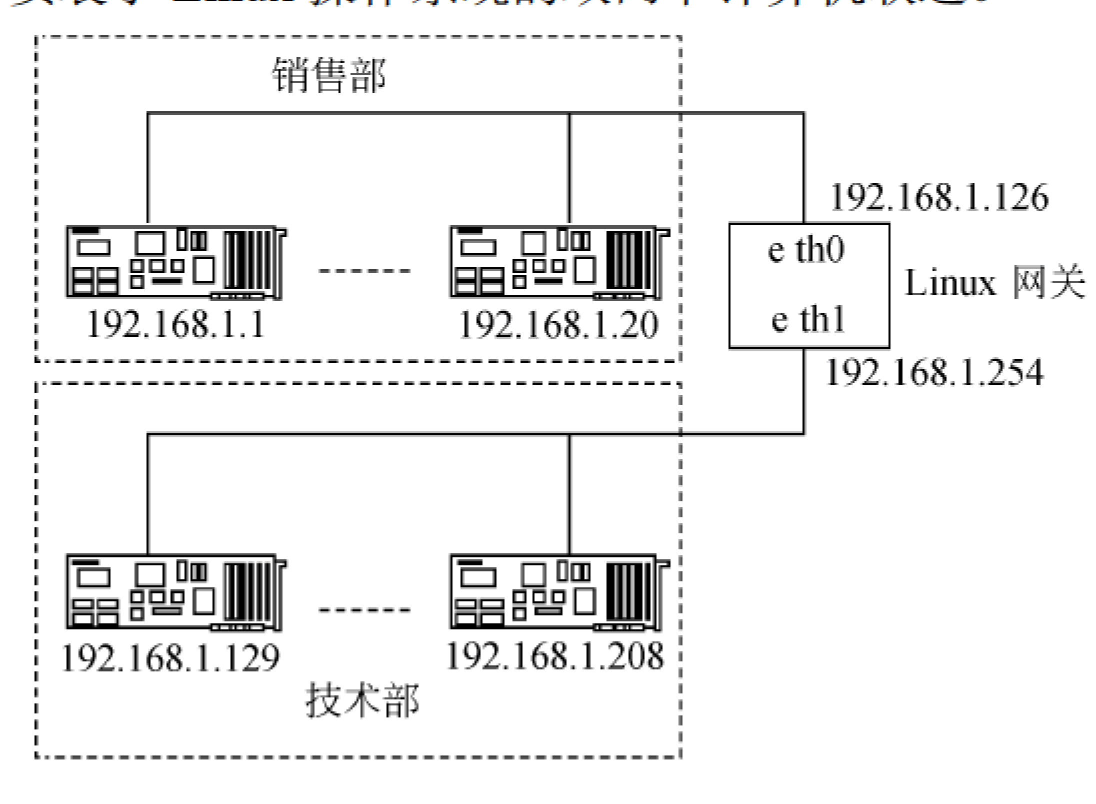


图 2-1

【问题 1】

销售部的网络号是__（1）__，广播地址是__（2）__；技术部的网络号是__（3）__，广播地址是__（4）__；每个子网可用的 IP 地址有__（5）__个。

【问题 2】

Linux 网关计算机有两个网络接口（eth0 和 eth1），每个接口与对应的子网相连接。该计算机/etc/sysconfig/network 文件清单为：

```
NETWORKING=yes
FORWARD_IPV4=（6）
HOSTNAME=gateway.ABC.com
/etc/sysconfig/network-scripts/ifcfg-eth0 文件清单为：
DEVICE=eth0
IPADDR=192.168.1.126
NETMASK=（7）
……（以下略）
/etc/sysconfig/network-scripts/ifcfg-eth1 文件清单为：
DEVICE=eth1
IPADDR=192.168.1.254
NETMASK=（8）
……（以下略）
```

（6）的备选答案：

A．yes　　B．no　　C．route　　D．gateway

【问题 3】

在网关计算机/etc/sysconfig/network-scripts/目录中有以下文件，运行某命令可以启动网络，该命令是__（9）__，其命令行参数是__（10）__。

```
ifcfg-eth0        ifup             ifup-sit
ifcfg-lo          ifup-aliases     ifup-si
ifdown            ifup-cipcb       ifup-wireless
ifdown-aliases    ifup-ippp        init. Ipv6-global
ifdown-cipcb      ifup-ipv6        network-functions
ifdown-ippp       ifup-ipx         network-functions-ipv6
ifdown-ipv6       ifup-isdn
ifdown-isdn       ifup-plip
ifdown-post       ifup-plusb
ifdown-ppp        ifup-post
ifdown-sit        ifup-ppp
ifdown-sl         ifup-routes
```

【问题 4】

在网关计算机上使用以下路由命令创建两个默认的路由：

```
route add -net 192.168.1.0    255.255.255.128   （11）
route add -net 192.168.1.128  255.255.255.128   （12）
```

【问题 5】

设置技术部和销售部的主机网络参数后，如果两个子网间的主机不能通信，用__(13)__命令来测试数据包是否能够到达网关计算机。如果数据包可以达到网关但是不能转发到目标计算机上，则需要用命令 cat /proc/sys/net/ipv4/ip_forward 来确认网关计算机的内核是否支持 IP 转发。如果不支持，该命令输出__(14)__。

（13）和（14）备选答案如下：

（13）A．traceroute　　B．tracert　　C．nslookup　　D．route

（14）A．1　　B．0　　C．yes　　D．no

试题二分析

【问题 1】

本题中图示的网络由一台双网卡的网关计算机均分成了两个子网，分别属于销售部和技术部，同部门的网络通信分别在各自的子网中进行，不同部门用户间的通信将由网关计算机进行转发，这样不再是所有的用户都在一个相同的、大型的网络上，子网划分的结果是提高了网络的速度。

整个网络的网络号是 192.168.1.0，是一个 C 类网络，子网掩码是 11111111.11111111.11111111.00000000（十进制表示为 255.255.255.0），即网络地址的前 3 个字节的每一位设置为 1，剩余的（主机地址）位设置为 0。当把剩余的表示主机地址的字节最高位设置为 1 时（即该位参与子网络的定义），网络就被均分成了两个子网，此时子网掩码为 11111111.11111111.11111111.10000000，用十进制表示为 255.255.255.128。

子网网络号可以用子网 IP 地址与子网掩码进行逐位 AND 运算得到。

销售部子网号：192.168.1.1（或 192.168.1.126）AND 255.255.255.128 等于 192.168.1.0；

技术部子网号：192.168.1.129（或 192.168.1.254）AND 255.255.255.128 等于 192.168.1.128。

对于销售部子网而言，主机号是 0 的地址（192.168.1.0）是子网地址，不能分配给主机，主机位全为 1 的地址（192.168.1.127）是子网广播地址，保留，也不能分配给主机；对于技术部子网而言，主机号是 0 的地址（192.168.1.128）是子网地址，不能分配给主机，主机位全为 1 的地址（192.168.1.255）是子网广播地址，保留，也不能分配给主机。因此这两个子网的可用 IP 地址是 126 个（128 减去 2 个保留地址）。

【问题 2】

Linux 计算机中，/etc/sysconfig/network 可配置文件定义了该计算机网络的基本属性，包括网络是否可用，是否允许 IP 包转发，主机域名，网关地址，网关设备名等。由于这台 Linux 计算机用于整个网络系统的网关，两个子网间的 IP 通信需要该计算机进行转发，因此文件中的 FORWARD_IPV4 应设置为“=”yes，就本题而言，即支持 IP 包在两个网卡设备间转发。如果要将 IP 包转发关闭，FORWARD_IPV4 应设置为“=”no。

网络接口文件/etc/sysconfig/network-scripts/ifcfg-eth0 定义了网络设备 eth0 的属性，由题目图示可知，该网络设备属于销售部子网，网络掩码为 255.255.255.128，即文件中的 NETMASK 应设置为“=”255.255.255.128；同样网络接口文件/etc/sysconfig/network-scripts/ifcfg-eth1 中的 NETMASK 应设置为“=”255.255.255.128。

【问题 3】

在/etc/sysconfig/network-scripts 目录中有许多脚本文件用于基本网络管理，包括启动网络设备、停止网络设备运行等。常用的两个脚本命令是 ifup 和 ifdown，前者是启动网络设备运行，后者是停止网络设备运行，脚本以设备名为参数，设备名为 eth0、eth1 等。

【问题 4】

当正确地配置了/etc/sysconfig/network 文件、/etc/sysconfig/network-scripts/ifcfg-eth0 文件和/etc/sysconfig/network-scripts/ifcfg-eth1 文件，并成功运行 ifup 脚本命令启动了 eth0 设备和 eth1 设备后，还需要在网关计算机上使用 route 命令分别为两个子网创建两个默认路由：

route add –net 192.168.1.0 255.255.255.128 eth0，销售部子网通过 eht0 转发；

route add –net 192.168.1.128 255.255.255.128 eth1，技术部子网通过 eht1 转发。

上面的路由命令确保把指定的网络传输的数据包通过指定的接口设备进行传输。

【问题 5】

两个子网间的主机要能够正常通信，首先应该正确设置技术部和销售部的主机网络参数，比如销售部的主机的网关地址应设置为 192.168.1.126，技术部的主机的网关地址应设置为 192.168.1.254。进行连通性测试常用的命令是 ping，当发现两个子网间的主机 ping 失败时，可以在网关计算机上使用 traceroute 命令来确定数据包是否能够达到网关的另一端。如果 traceroute 显示数据可以到达网关但是不能转发到目标计算机上，问题就出现在网关上。应该保证 IP 转发在网关计算机上是允许的，在网关计算机上运行 cat /proc/sys/net/ipv4/ip_forward，查询内核的 IP 转发参数，如果返回的是 0，说明 IP 转发在内核中是禁止的，此时需要重新编译内核，使内核支持 IP 转发，即 cat /proc/sys/net/ipv4/ip_forward 的返回为 1。

参考答案

【问题 1】

（1）192.168.1.0

（2）192.168.1.127

（3）192.168.1.128

（4）192.168.1.255

（5）126

【问题 2】

（6）A 或 yes

（7）255.255.255.128

（8）255.255.255.128

【问题 3】

（9）ifup

（10）网络接口（或设备）名称（或 eth0 或 eth1）

【问题 4】

（11）eth0

（12）eth1

【问题 5】

（13）A 或 traceroute

（14）B 或 0

试题三（15 分）

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】

通过 SNMP 可以获得网络中各种设备的状态信息，还能对网络设备进行控制。在 Windows Server 2003 中可以采用 IPSec 来保护 SNMP 通信，配置管理站的操作步骤为：先创建筛选器，对输入的分组进行筛选，然后创建 IPSec 策略。

【问题 1】

在“管理工具”中运行“管理 IP 筛选器列表”，创建一个名为“SNMP 消息”的筛选器。在如图 3-1 所示的“IP 筛选器向导”中指定 IP 通信的源地址，下拉列表框中应选择__（1）__；在如图 3-2 中指定 IP 通信的目标地址，下拉列表框中应选择__（2）__。

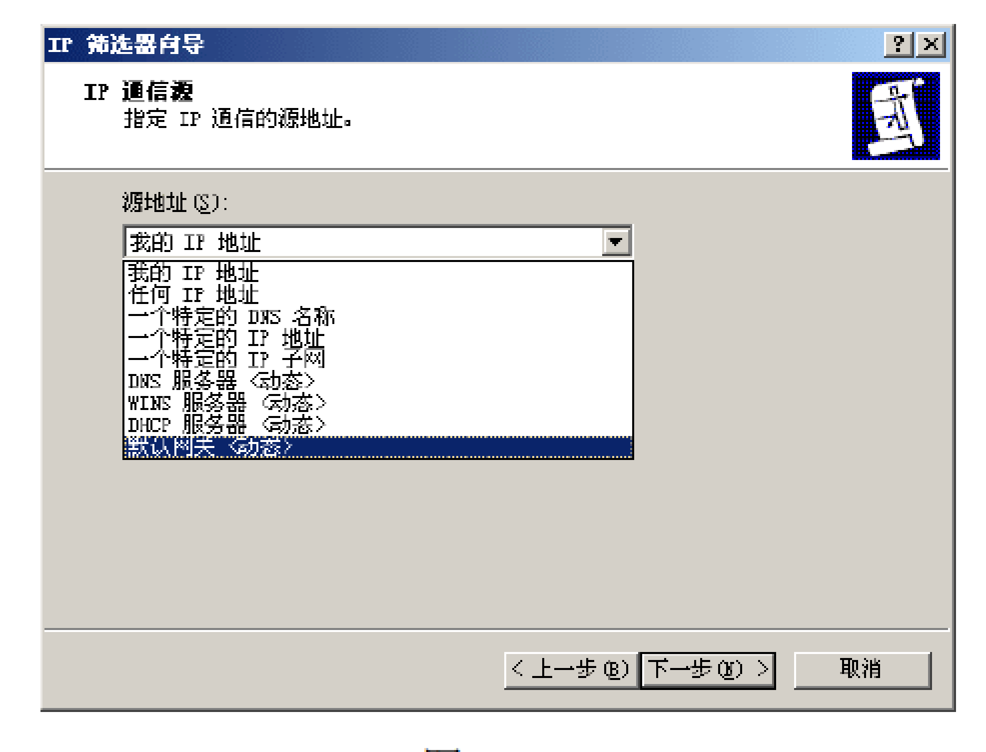


图 3-1

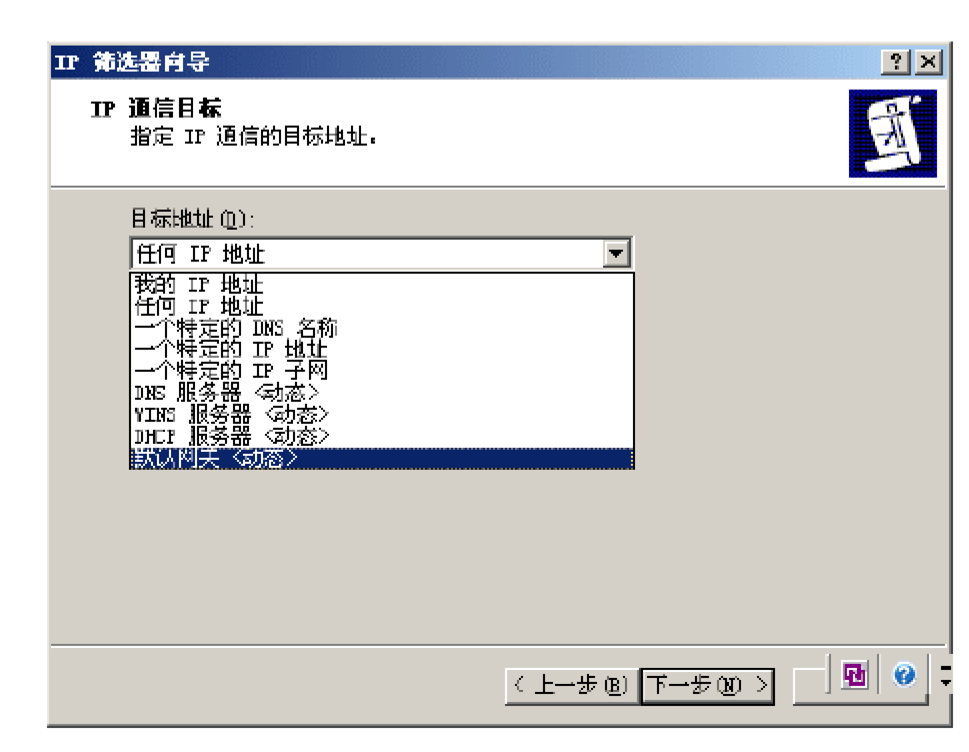


图 3-2

在图 3-3 所示的“选择协议类型”下拉列表框中应选择__（3）__。

对于 SNMP 协议，在图 3-4 中设置“从此端口”项的值为__（4）__，“到此端口”项的值为__（5）__；对于 SNMP TRAP 协议，在图 3-4 中设置“从此端口”项的值为__（6）__，

“到此端口”项的值为__（7）__。

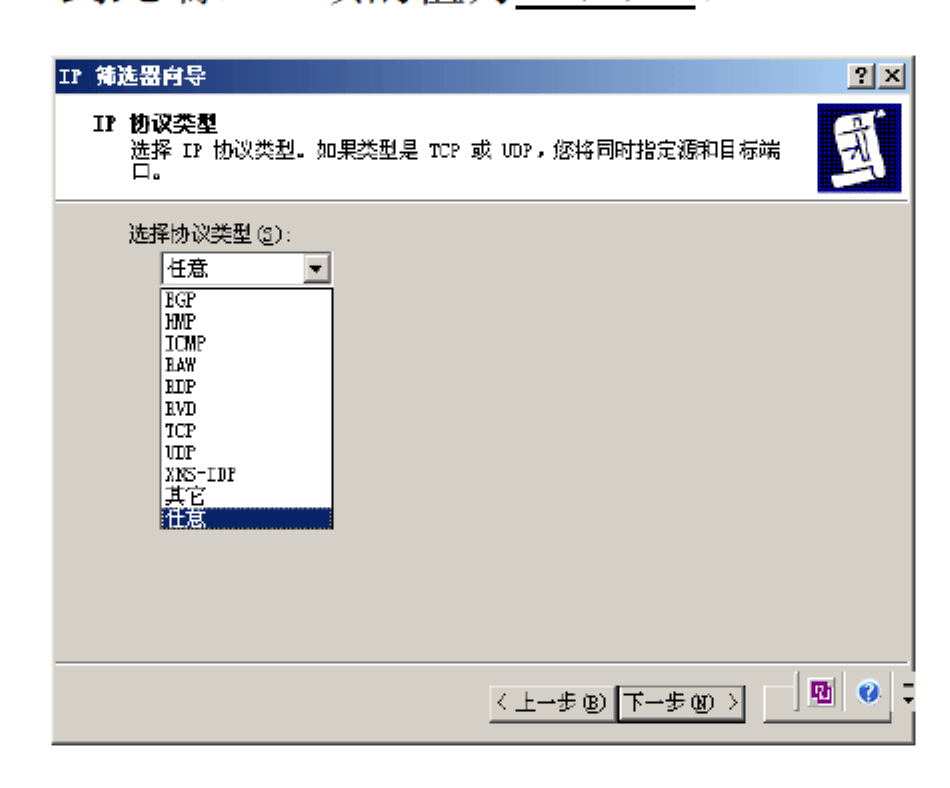


图 3-3

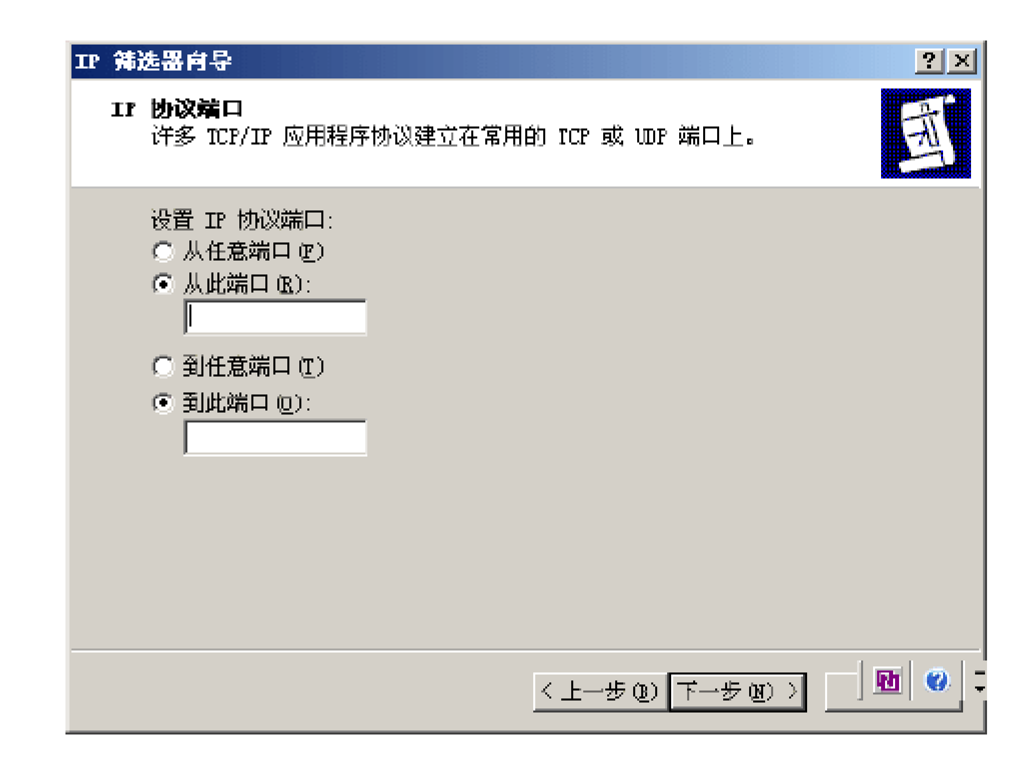


图 3-4

【问题 2】

在创建 IPSec 安全策略时，规则属性窗口如图 12-5 所示。在“IP 筛选器列表”中应选择__（8）__。

【问题 3】

在“新规则属性”对话框中打开“筛选器操作”选项卡，选择“Permit”，在图 3-6 中应选择__（9）__，同时选中“接受不安全的通讯，但总是使用 IPSec 响应（C）”和“使用会话密钥完全向前保密（PFS）（K）”复选框。

（9）的备选答案：

A．许可　　B．阻止　　C．协商安全

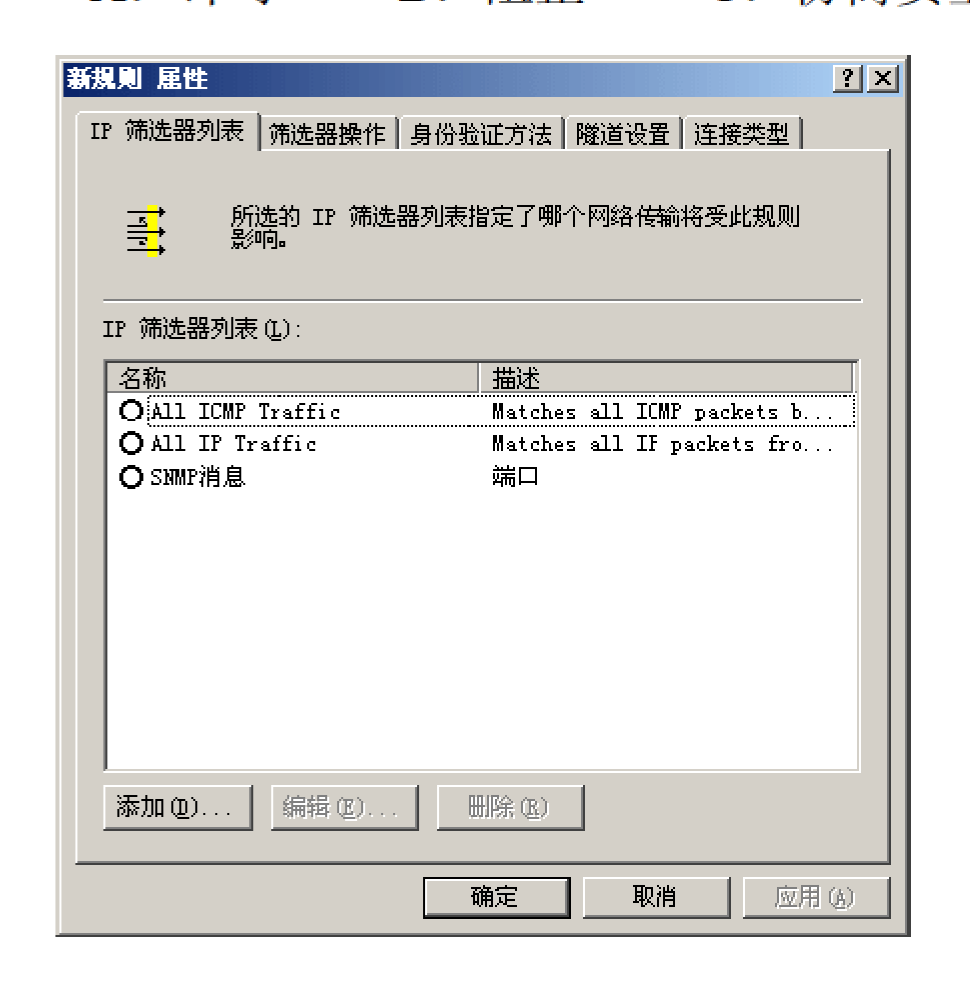


图 3-5

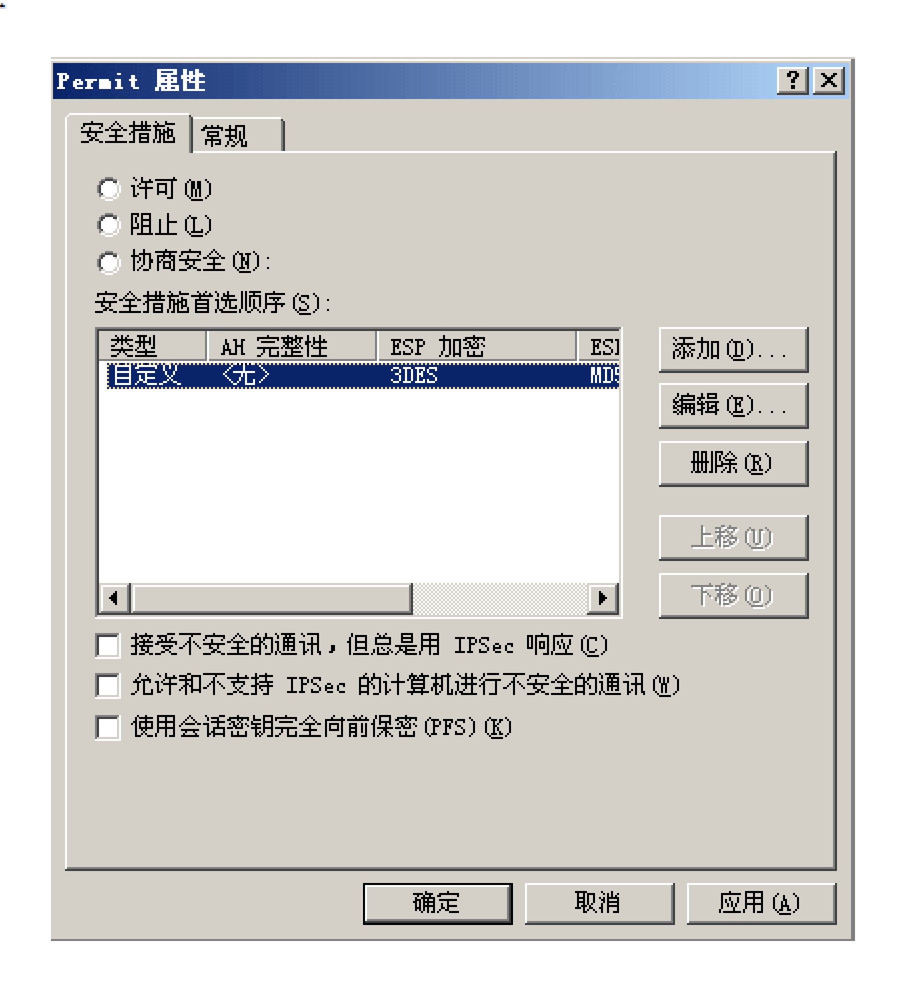


图 3-6

【问题 4】

在图 3-7 所示的密钥交换设置对话框中，选中“主密钥完全向前保密（PFS）（P）”复选框，则“身份验证和生成新密钥间隔”默认值为 480 分钟和 ＿（10）＿个会话。

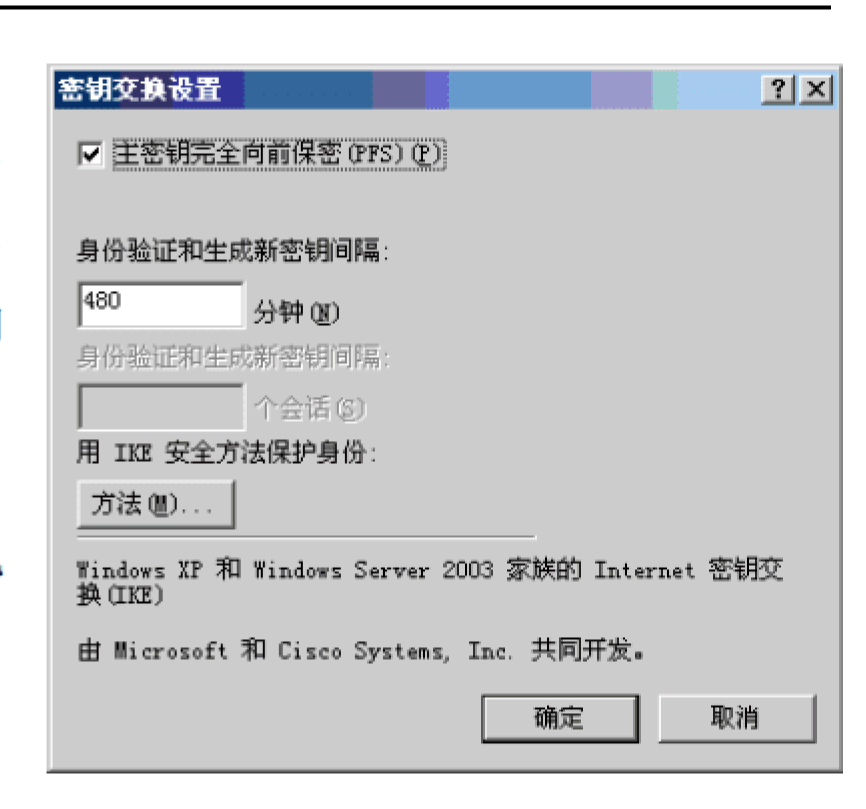


图 3-7

【问题 5】

为保证 SNMP 正常通信，被管理的其他计算机应如何配置？

试题三分析

【问题 1】

管理站对输入的 SNMP 消息进行筛选时，目的地址为本机地址，源地址为本站管理的任意 IP 地址，因此（1）应填入“任何 IP 地址”，（2）应填入“我的 IP 地址”。

采用 SNMP 进行网络管理时，传输层采用 UDP，故（3）应填入“UDP”。

由于 SNMP 协议默认端口为 161，故（4）、（5）依次应填入 161、161；SNMP TRAP 协议默认端口为 162，故（6）、（7）依次应填入 162、162。

【问题 2】

由于创建的筛选器名为“SNMP 消息”，因此应针对该筛选器创建 IPSec 安全策略，故（8）应选择“SNMP 消息”。

【问题 3】

管理站和被管站之间应采用协商方式进行安全通信，因此（9）应填入“协商安全”或选择 B。

【问题 4】

主密钥完全向前保密（PFS），每次都强制使用新“材料”重新生成密钥。若选中“主密钥完全向前保密（PFS）”复选框，则“身份验证和生成新密钥间隔”默认值为 480 分钟和 1 个会话。

因此（10）应填入“1”。

【问题 5】

为保证 SNMP 正常通信，被管理的其他计算机上必须配置相应的 IPSec 安全策略，否则无法保障安全。

参考答案

【问题 1】

（1）任何 IP 地址

（2）我的 IP 地址

（3）UDP

（4）161

（5）161

（6）162

（7）162

【问题 2】

（8）SNMP 消息

【问题 3】

（9）C 或协商安全

【问题 4】

（10）1

【问题 5】

其他计算机上必须配置相应的 IPSec 安全策略。

试题四（15 分）

阅读以下说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。

【说明】

某公司在 Windows Server 2003 中安装 IIS 6.0 来配置 Web 服务器，域名为 www.abc.com。

【问题 1】

IIS 安装的硬盘分区最好选用 NTFS 格式，是因为__（1）__和__（2）__。

A．可以针对某个文件或文件夹给不同的用户分配不同的权限

B．可以防止网页中的 Applet 程序访问硬盘中的文件

C．可以使用系统自带的文件加密系统对文件或文件夹进行加密

D．可以在硬盘分区中建立虚拟目录

【问题 2】

为了禁止 IP 地址为 202.161.158.239~202.161.158.254 的主机访问该网站，在图 4-1 所示的“IP 地址和域名限制”对话框中单击“添加”按钮，增加两条记录，如表 4-1 所示。填写表 4-1 中的（3）～（5）处内容。

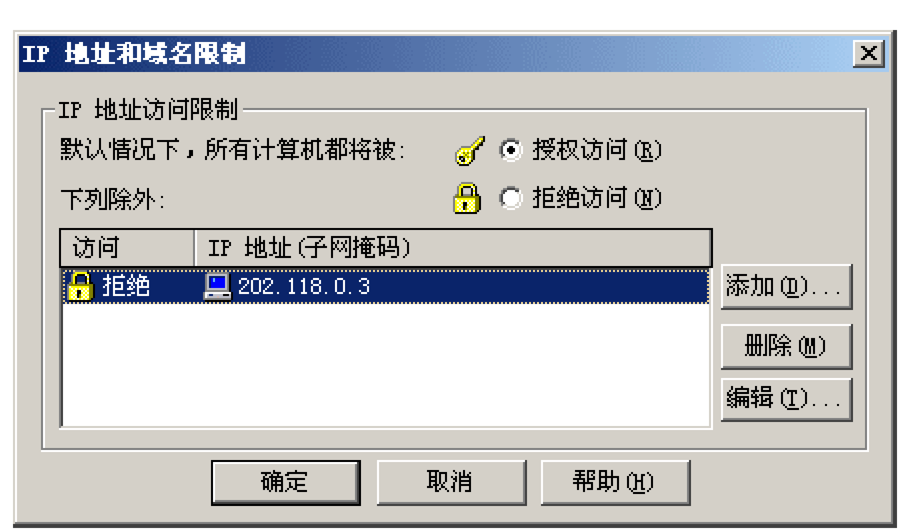


图 4-1

表 4-1

	IP 地址	子网掩码
一组主机	（3）	（4）
一台主机	（5）	

【问题 3】

实现保密通信的 SSL 协议工作在 HTTP 层和__(6)__层之间。SSL 加密通道的建立过程如下：

1．首先客户端与服务器建立连接，服务器把它的__(7)__发送给客户端；

2．客户端随机生成__(8)__，并用从服务器得到的公钥对它进行加密，通过网络传送给服务器；

3．服务器使用__(9)__解密得到会话密钥，这样客户端和服务器端就建立了安全通道。

（6）～（9）的备选答案如下：

A．TCP　B．IP　C．UDP　D．公钥　E．私钥

F．对称密钥　G．会话密钥　H．数字证书　I．证书服务

【问题 4】

在 IIS 中安装 SSL 分 5 个步骤，这 5 个步骤的正确排序是__(10)__。

A．配置身份验证方式和 SSL 安全通道

B．证书颁发机构颁发证书

C．在 IIS 服务器上导入并安装证书

D．从证书颁发机构导出证书文件

E．生成证书请求文件

【问题 5】

在安装 SSL 时，在“身份验证方法”对话框中应选用的登录验证方式是__(11)__。

A．匿名身份验证　B．基本身份验证

C．集成 Windows 身份验证　D．摘要式身份验证

E．.Net Passport 身份验证

【问题 6】

如果用户需要通过 SSL 安全通道访问该网站，应该在 IE 的地址栏中输入__(12)__。SSL 默认侦听的端口是__(13)__。

试题四分析

【问题 1】

为了确保 IIS 服务的安全，一个重要的前提就是让它落地在安全的系统上。在 Windows 服务器上安装 IIS 最好选用 NTFS 分区格式。因为在 NTFS 格式下，可以针对某个文件或文件夹给不同的用户分配不同的权限，并且可以使用系统自带的加密文件系统 EFS 对文件夹或文件进行加密。

【问题 2】

在 IIS 中，如果发现来自某一 IP 的计算机总是试图攻击网站，就可以使用“IP 地址及域名限制”来禁止其访问。通过 IP 地址及其域名限制，用户可以禁止某些特定的计算

机或某个地址段中的计算机对子集的 Web 和 FTP 站点的访问。当有大量的攻击和破坏来自于某些地址或某个子网时，使用这种限制机制是非常有用的。

为了禁止 IP 地址为 202.161.158.239～202.161.158.254 的主机访问该网站，可以将这个地址段中的所有 IP 地址以单个主机的形式加入限制访问的地址列表中，也可以以 IP 地址加子网掩码的形式添加一组主机地址。这里如果采用子网掩码，那么 202.161.158.239 不在该网段，还需要单独添加该主机 IP。

【问题 3】

本问题考查的是 SSL 安全加密机制的基础知识。SSL 是一个协议独立的加密方案，在网络信息包的应用层和传输层之间提供了安全的通道。

【问题 4】

IIS 使用的是 HTTP 协议，以明文的形式传输数据，没有采用任何加密手段，传输的重要数据容易被窃取。如果建立了 SSL 安全机制，只有 SSL 允许的客户才能与 SSL 允许的 Web 站点进行通信。

在 Windows Server 2003 中，为 IIS 安装 SSL 安全加密机制需要以下步骤：

（1）生成证书请求文件；

（2）安装证书服务；

（3）申请 IIS 网站证书；

（4）颁发 IIS 网站证书；

（5）导入 IIS 网站证书；

（6）配置 IIS 安全通信。

【问题 5】

导入证书后，IIS 并没有启用 SSL 安全加密功能，需要进一步对 IIS 服务器进行配置。在“目录安全性”选项卡中单击“安全通信”中的“编辑”按钮，弹出“安全通信”对话框，从中选择“要求安全通道（SSL）”和“要求 128 位加密”。接着单击“身份验证和访问控制”的“编辑”按钮，弹出“身份验证方法”对话框，取消选中“启用匿名访问”和“集成 Windows 身份验证”复选框，只选中“基本身份验证”复选框即可。

【问题 6】

使用安装的 SSL 安全加密机制的 Web 站点，需要在使用 URL 资源定位器时要输入 https://。

参考答案

【问题 1】

（1）A　（2）C

【问题 2】

（3）202.161.158.240 至 202.161.158.254 均可

（4）255.255.255.240

（5）202.161.158.239

【问题 3】

（6）A；（7）H；（8）G；（9）E

【问题 4】

（10）EBDCA

【问题 5】

（11）B

【问题 6】

（12）https://www.abc.com；（13）443

试题五（15 分）

阅读下面的说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某企业园区网采用了三层架构，按照需求，在网络中需要设置 VLAN、快速端口、链路捆绑、Internet 接入等功能。该园区网内部分 VLAN 和 IP 地址如表 5-1 所示。

表 5-1

VLAN 号	VLAN 名称	IP 网段	默认网关	说　　明
Vlan1		192.168.1.0/24	192.168.1.254	管理 Vlan
Vlan10	Xsb	192.168.10.0/24	192.168.10.254	销售部 Vlan
Vlan20	Scb	192.168.20.0/24	192.168.20.254	生产部 Vlan
Vlan30	Sjb	192.168.30.0/24	192.168.30.254	设计部 Vlan
Vlan50	Fwq	192.168.50.0/24	192.168.50.254	服务器 Vlan

【问题 1】

某交换机的配置命令如下，根据命令后面的注释，填写（1）～（3）处的空缺内容，完成配置命令。

```
Switch(config)# (1)                  //将交换机命名为 Sw1
Sw1(config)# interface vlan 1
Sw1(config-if)# (2)                  //设置交换机的 IP 地址为 192.168.1.1/24
Sw1(config-if)# no shutdown
Sw1(config)# (3)                     //设置交换机默认网关地址
```

【问题 2】

在核心交换机中设置了各个 VLAN，在交换机 Sw1 中将端口 1～20 划归销售部，请完成以下配置。

```
Sw1(config)# interface range fastethernet0/1-20//进入组配置状态
Sw1(config-if-range)# (4)            //设置端口工作在访问（接入）模式
Sw1(config-if-range)# (5)            //设置端口 1～20 为 VLAN 10 的成员
```

【问题 3】

1．在默认情况下，交换机刚加电启动时，每个端口都要经历生成树的四个阶段，它们分别是：阻塞、侦听、__（6）__、__（7）__。

2．根据需求，需要将 Sw1 交换机的端口 1～20 设置为快速端口，完成以下配置。

```
Sw1(config)# interface range fastethernet0/1-20//进入组配置状态
Sw1(config-if-range)#__(8)__                   //设置端口 1～20 为快速端口
```

【问题 4】

该网络的 Internet 接入如图 5-1 所示：

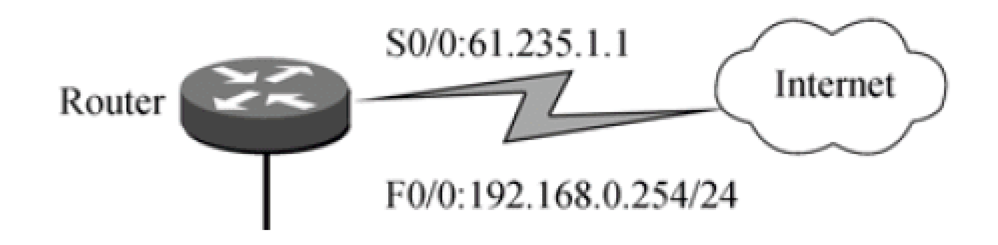


图 5-1

根据图 5-1，解释以下配置命令，填写空格（9）～（12）：

```
1. Router(config)# interface s0/0
2. router(config-if)#ip address 61.235.1.1 255.255.255.252     __(9)__
3. router(config)#ip route 0.0.0.0 0.0.0.0 s0/0                __(10)__
4. router(config)#ip route 192.168.0.0 255.255.255.0 f0/0      __(11)__
5. router(config)#access-list 100 deny any any eq telnet       __(12)__
```

试题五分析

【问题 1】

本问题考查的是交换机的基本配置命令，包括设置交换机的名称，配置交换机的 IP 地址和默认网关。参照题目要求，该交换机的名称为 Sw1，IP 地址为 192.168.1.1/24，根据表 5-1 可知其默认网关为 192.168.1.254。故其配置命令为：

```
Switch(config)# hostname sw1
Sw1(config)# interface vlan 1
Sw1(config-if)# ip address 192.168.1.1 255.255.255.0
Sw1(config-if)# no shutdown
Sw1(config)# ip default-gateway 192.168.1.254
```

【问题 2】

本问题考查的是端口 vlan 配置的命令。参照题目要求，交换机 Sw1 中将端口 1～20 划归销售部，而销售部是 vlan 10，另外根据题目提示，配置采用组配置模式。故其配置命令为：

```
Sw1(config)# interface range fastethernet0/1-20
Sw1(config-if-range)# switchport mode access
Sw1(config-if-range(# switchport access vlan 10
```

【问题 3】

本问题考查的是生成树基本概念和快速端口配置。默认情况下，交换机在刚加电启动时，每个端口都要经历生成树的四个阶段：阻塞、侦听、学习和转发。在能够转发用户的数据包之前，某个端口可能最多要等 50s 的时间（20s 的阻塞时间+15s 的侦听延迟时间+15s 的学习延迟时间）。

对于直接接入终端工作站的端口来说，用于阻塞和侦听的时间是不必要的。为了加速交换机端口状态转化时间，可以利用 spanning-tree portfast 命令将某端口设置成为快速端口（Portfast）。设置为快速端口的端口后，当交换机启动或端口有工作站接入时，将会直接进入转发状态，而不会经历阻塞、侦听和学习状态（假设桥接表已经建立）。

【问题 4】

本问题考查的是广域网接入路由器的配置命令。

```
1. Router(config)# interface s0/0
```

该命令是进入串口配置模式。

```
2. router(config-if)#ip address 61.235.1.1 255.255.255.252
```

该命令的作用是设置串口的 IP 地址及子网掩码。

```
3. router(config)#ip route 0.0.0.0 0.0.0.0 s0/0
```

该命令的作用是设置到 Internet 的默认路由。

```
4. router(config)#ip route 192.168.0.0 255.255.255.0 f0/0
```

该命令的作用是设置到校园网内部的路由。

```
5. router(config)#access-list 100 deny any any eq telnet
```

该命令的作用是定义屏蔽远程登录协议 telnet 的规则。

参考答案

【问题 1】

（1）hostname sw1

（2）ip address 192.168.1.1 255.255.255.0

（3）ip default-gateway 192.168.1.254

【问题 2】

（4）switchport mode access

（5）switchport access vlan 10

【问题 3】

（6）学习

（7）转发

以上两个答案可以互换

（8）spanning-tree portfast

【问题 4】

（9）设置串口的 IP 地址及子网掩码

（10）设置到 Internet 的默认路由

（11）设置到校园网内部的路由

定义屏蔽远程登录协议 telnet 的规则

第 11 章　2007 上半年网络工程师上午试题分析与解答

试题（1）

__（1）__不属于计算机控制器中的部件。

（1）A．指令寄存器 IR　　　　　　　B．程序计数器 PC

　　C．算术逻辑单元 ALU　　　　　　D．程序状态字寄存器 PSW

试题（1）分析

本题考查的是计算机系统硬件方面的基础知识。构成计算机控制器的硬件主要有指令寄存器 IR、程序计数器 PC、程序状态字寄存器 PSW、时序部件和微操作形成部件等。而算术逻辑单元 ALU 不是构成控制器的部件。

参考答案

（1）C

试题（2）

在 CPU 与主存之间设置高速缓冲存储器（Cache），其目的是为了__（2）__。

（2）A．扩大主存的存储容量　　　　　B．提高 CPU 对主存的访问效率

　　C．既扩大主存容量又提高存取速度　D．提高外存储器的速度

试题（2）分析

为了提高 CPU 对主存的存取速度，又不至于增加很大的价格。现在，通常在 CPU 与主存之间设置高速缓冲存储器（Cache），其目的就在于提高速度而不增加很大代价。同时，设置高速缓冲存储器并不能增加主存的容量。

参考答案

（2）B

试题（3）

下面的描述中，__（3）__不是 RISC 设计应遵循的设计原则。

（3）A．指令条数应少一些

　　B．寻址方式尽可能少

　　C．采用变长指令，功能复杂的指令长度长而简单指令长度短

　　D．设计尽可能多的通用寄存器

试题（3）分析

本题考查的是计算机系统硬件方面的基础知识。在设计 RISC 时，需要遵循如下一些基本的原则。

① 指令条数少，一般为几十条指令。

② 寻址方式尽可能少。

③ 采用等长指令，不管功能复杂的指令还是简单的指令，均用同一长度。

④ 设计尽可能多的通用寄存器。

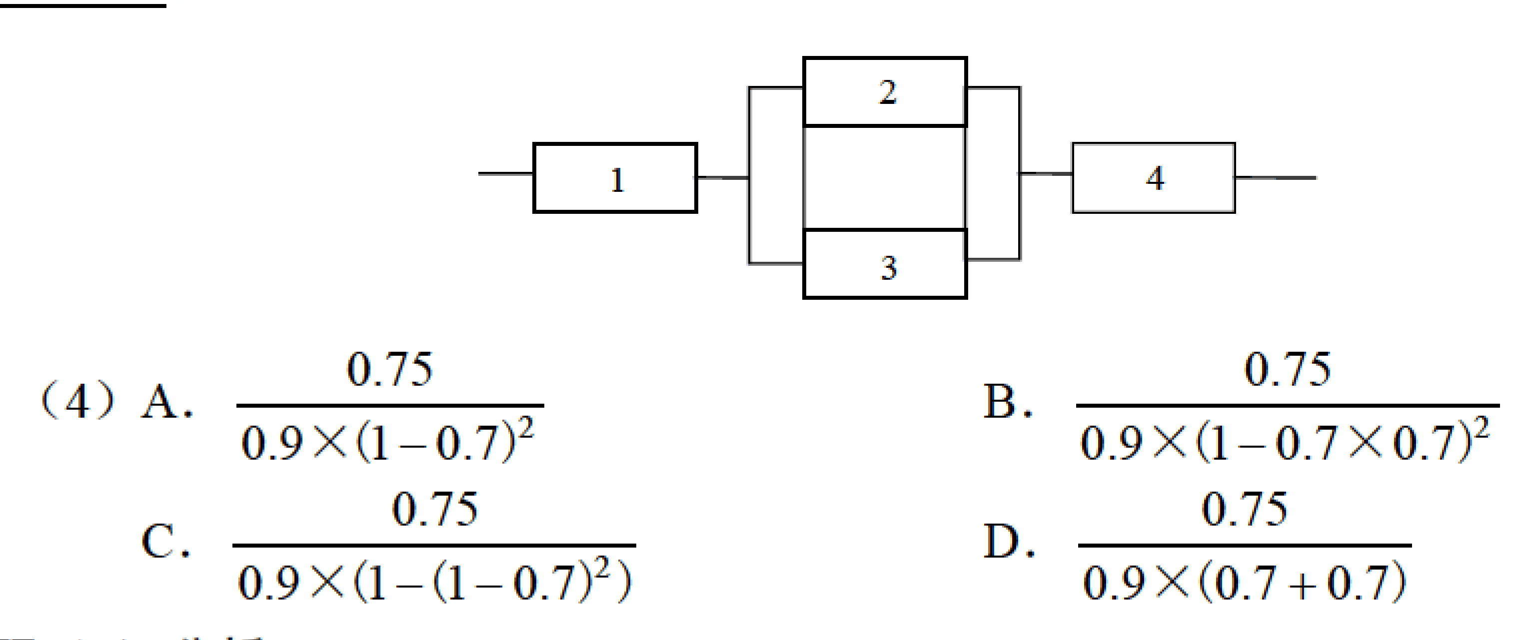
因此，采用变长指令，功能复杂的指令长度长而简单指令长度短不是应采用的设计原则。

参考答案

（3）C

试题（4）

某系统的可靠性结构框图如下图所示。该系统由 4 个部件组成，其中 2、3 两部件并联冗余，再与 1、4 部件串联构成。假设部件 1、2、3 的可靠度分别为 0.90、0.70、0.70。若要求该系统的可靠度不低于 0.75，则进行系统设计时，分配给部件 4 的可靠度至少应为 （4） 。



（4）A. $\frac{0.75}{0.9\times(1-0.7)^2}$　　B. $\frac{0.75}{0.9\times(1-0.7\times0.7)^2}$

C. $\frac{0.75}{0.9\times(1-(1-0.7)^2)}$　　D. $\frac{0.75}{0.9\times(0.7+0.7)}$

试题（4）分析

本题考查的是计算机系统硬件方面的基础知识。从可靠性设计角度分析，该试题给出的是一种串并混合系统。首先考虑部件 2 和部件 3 是并联冗余结构，它们的可靠度分别为 0.70，两者并联冗余的可靠度为 $1-(1-0.70)^2=0.91$。在此基础上，系统可以看作是可靠度为 0.90 的部件 1、可靠度为 0.91 的冗余部件和部件 4 串联构成，串联系统的可靠度为各部件可靠度之积，要求构成的系统的可靠度不低于 0.75。若设部件 4 的可靠度为 R_4，则

$$0.9\times(1-(1-0.70)^2)\times R_4=0.75$$

从而可以由下式求出部件 4 的可靠度 $R_4=\frac{0.75}{0.9\times(1-(1-0.7)^2)}$

参考答案

（4）C

试题（5）

结构化开发方法中，数据流图是 （5） 阶段产生的成果。

（5）A. 需求分析　　B. 总体设计　　C. 详细设计　　D. 程序编码

试题（5）分析

结构化分析是面向数据流进行需求分析的方法，数据流图是分析过程中用来描述数据处理过程的工具，它从数据传递和加工的角度，以图形的方式刻画数据流从输入到输出的移动变换过程，是对软件所要处理数据的抽象。由于数据流图只反映系统必须完成的逻辑功能，所以它是一种功能模型。

参考答案

（5）A

试题（6）

关于原型化开发方法的叙述中，不正确的是__（6）__。

（6）A．原型化方法适应于需求不明确的软件开发

B．在开发过程中，可以废弃不用早期构造的软件原型

C．原型化方法可以直接开发出最终产品

D．原型化方法利于确认各项系统服务的可用性

试题（6）分析

原型化软件开发方法的基本思想是软件开发人员对用户提出的需求和问题进行总结，就系统的主要需求取得一致意见后，构造一个软件原型（原型是软件的一个早期版本，通常反映最终软件的部分重要特性，原型应该是可以运行和修改的），使用户在试用原型过程中得到感受和启发，并做出反应和评价。然后开发者根据用户的意见对原型进行改进，使之逐步完善，直到用户对系统完全满意为止。这种开发方法的优点是需求表示清楚，用户满意度较高、可降低开始风险和开发成本。所以原型化方法特别适应于原始需求不明确的软件，因为通过用户的不断使用和体验并提出评价，使得不断修改的原型逐步达到用户要求。通常，软件开发过程中会得到多个软件原型，只有得到用户认可的才是最终的产品。

参考答案

（6）C

试题（7）

如果两名以上的申请人分别就同样的发明创造申请专利，专利权应授予__（7）__。

（7）A．最先发明的人　B．最先申请的人　C．所有申请人　D．协商后的申请人

试题（7）分析

根据我国专利法第九条规定“两个以上的申请人分别就同样的发明创造申请专利的，专利权授予最先申请的人。”，针对两名以上的申请人分别就同样的发明创造申请专利，专利权应授予最先申请的人。

参考答案

（7）B

试题（8）

CMM 模型将软件过程的成熟度分为 5 个等级。在＿（8）＿使用定量分析来不断地改进和管理软件过程。

（8）A．优化级　　B．管理级　　C．定义级　　D．可重复级

试题（8）分析

CMM 为软件企业的过程能力提供了一个阶梯式的进化框架，将软件过程改进的进化步骤组织成 5 个成熟度等级，每一个级别定义了一组过程能力目标，并描述了要达到这些目标应该采取的实践活动，为不断改进过程奠定了循序渐进的基础。

在初始级，企业一般缺少有效的管理，不具备稳定的软件开发与维护的环境。软件过程是未加定义的随意过程，项目的执行随意甚至是混乱的，几乎没有定义过程的规则（或步骤）。

在可重复级，企业建立了基本的项目管理过程的政策和管理规程，对成本、进度和功能进行监控，以加强过程能力。

在定义级，企业全面采用综合性的管理及工程过程来管理，对整个软件生命周期的管理与工程化过程都已标准化，并综合成软件开发企业标准的软件过程。

在管理级，企业开始定量地认识软件过程，软件质量管理和软件过程管理是量化的管理。对软件过程与产品质量建立了定量的质量目标，制定了软件过程和产品质量的详细而具体的度量标准，实现了度量标准化。

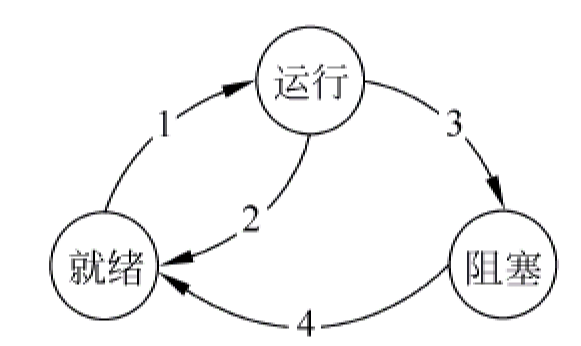
在优化级，企业将会把工作重点放在对软件过程改进的持续性、预见及增强自身，防止缺陷及问题的发生，不断地提高过程处理能力上。通过来自过程执行的质量反馈和吸收新方法和新技术的定量分析来改善下一步的执行过程，即优化执行步骤，使软件过程能不断地得到改进。

参考答案

（8）A

试题（9）

某系统的进程状态转换如下图所示，图中 1、2、3 和 4 分别表示引起状态转换的不同原因，原因 4 表示＿（9）＿。



（9）A．就绪进程被调度　　B．运行进程执行了 P 操作

C．发生了阻塞进程所等待的事件　　D．运行进程的时间片到了

试题（9）分析

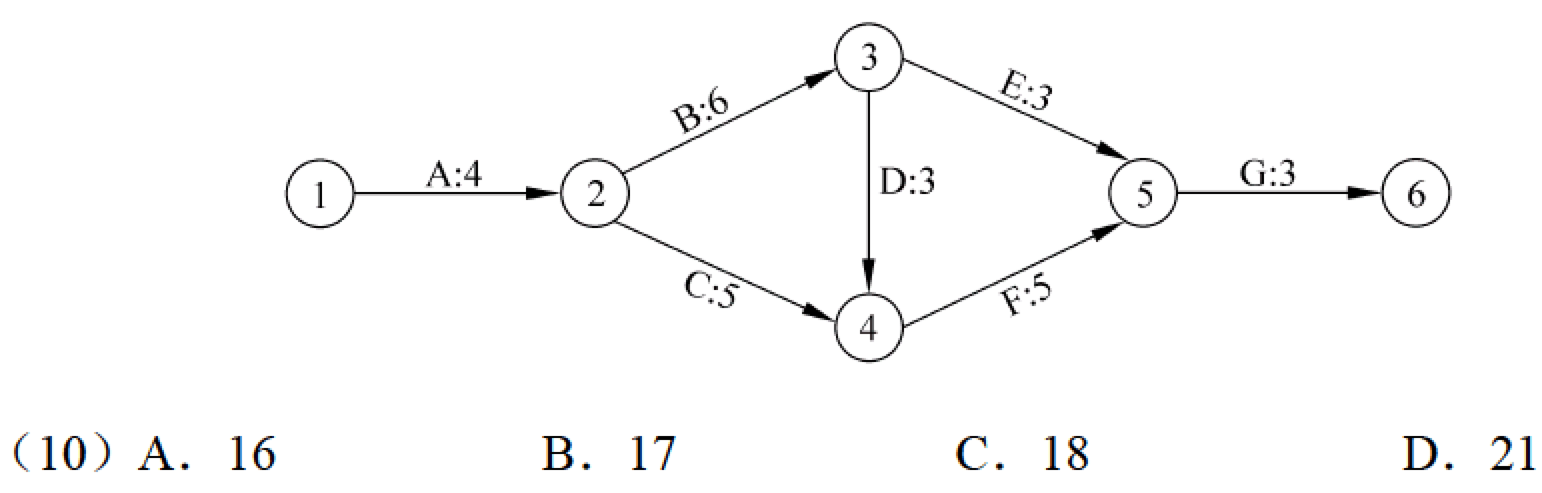
本题考查的是计算机操作系统进程管理方面的基础知识。图中原因 1 是由于调度程序的调度引起；原因 2 是由于时间片用完引起；原因 3 是由于 I/0 请求引起，例如进程执行了 P 操作，由于申请的资源得不到满足进入阻塞队列；原因 4 是由于 I/O 完成引起的，例如某进程执行了 V 操作将信号量值减 1，若信号量的值小于 0，意味着有等待该资源的进程，将该进程从阻塞队列中唤醒使其进入就绪队列；因此试题（9）的正确答案是 C。

参考答案

（9）C

试题（10）

某网络工程计划图如下所示，边上的标记为任务编码及其需要的完成时间（天），则整个工程的工期为__（10）__。



（10）A．16　　B．17　　C．18　　D．21

试题（10）分析

本题主要考查项目管理中进度管理中的网络图方面的知识。题目给出的工程网络图表示各个任务完成需要的时间以及相互依存的关系，整个工程的工期就是网络图中关键路径上各个任务完成时间的总和。就本题而言，关键路径是①-②-③-④-⑤-⑥，历时 21 天。

参考答案

（10）D

试题（11）

关于多模光纤，下面的描述中错误的是__（11）__。

（11）A．多模光纤的芯线由透明的玻璃或塑料制成

B．多模光纤包层的折射率比芯线的折射率低

C．光波在芯线中以多种反射路径传播

D．多模光纤的数据速率比单模光纤的数据速率高

试题（11）分析

光纤传输介质由可以传送光波的玻璃纤维或透明塑料制成，外包一层比玻璃折射率低的材料。进入光纤的光波在两种材料的界面上形成全反射，从而不断地向前传播。

光波在光导纤维中以多种模式传播，不同的传播模式有不同的电磁场分布和不同的传播路径，这样的光纤叫多模光纤。光波在光纤中以什么模式传播．这与芯线和包层的相对折射率、芯线的直径以及工作波长有关。如果芯线的直径小到光波波长大小，则光纤就成为波导，光在其中无反射地沿直线传播，这种光纤叫单模光纤。单模光纤比多模光纤的数据速率高，但价格更昂贵。单模光纤与多模光纤的传播模式如图 1 所示。

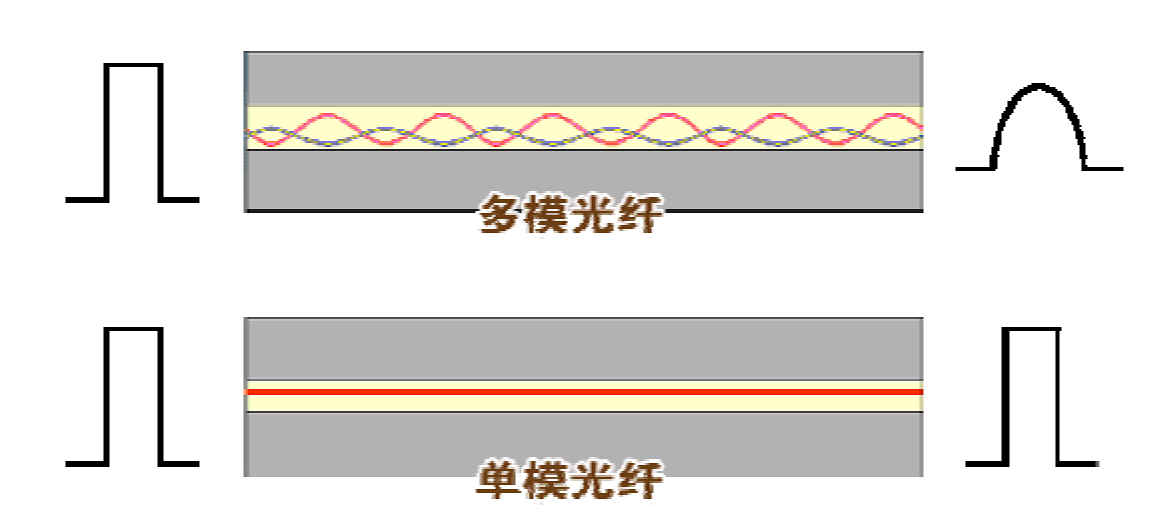


图 1　多模光纤与单模光纤传播模式

光导纤维作为传输介质，其优点是很多的。首先是它具有很高的数据速率、极宽的频带、低误码率和低延迟。典型数据速率是 100 Mb/s，甚至可达 1000 Mb/s，而误码率比同轴电缆可低两个数量级，只有 10^{-9}。其次是光传输不受电磁干扰，不可能被偷听，因而安全和保密性能好。最后，光纤重量轻、体积小、铺设容易。

参考答案

（11）D

试题（12）

关于路由器，下列说法中错误的是__（12）__。

（12）A．路由器可以隔离子网，抑制广播风暴

B．路由器可以实现网络地址转换

C．路由器可以提供可靠性不同的多条路由选择

D．路由器只能实现点对点的传输

试题（12）分析

路由器是网络层设备，它可以起到隔离子网、抑制广播风暴的作用。路由器还能进行地址转换，通常用于把私网地址转换成公网地址，或者进行相反的转换。在路由表中，对于同一目标，可以设置不同的通路，提供不同的服务。IPv4 数据报头的第二个字节（如图 2 所示）是服务类型字段（Type of Service）。该字段规定了不同的优先级（Precedence），延迟（Delay），吞吐率（Throughput）和可靠性（Reliability），为上层协议提供不同的服务质量。IP 数据报中的目标地址（Destination address）字段可以是广播地址、组播地址和单播地址，当目标地址为前两种类型时，路由器可以实现点到多点的传输。

Version IHL Type of Service Total Length

Identification Flags Fragment Offset

Time to Live Protocol Header Checksum

Source address

Destination address

Option + Padding

Data

图 2 IP 数据报的格式

参考答案

（12）D

试题（13）

100Base-FX 采用 4B/5B 和 NRZ-I 编码，这种编码方式的效率为__（13）__。

（13）A．50%　　B．60%　　C．80%　　D．100%

试题（13）分析

在快速以太网中，不能使用曼彻斯特编码。因为曼码的编码效率是 50%，即 100Mb/s 的数据速率要求 200M 的波特率。为了提高编码的效率，降低电路的频率（成本），在高速网络中采用 4B/5B 编码法，这种编码方法的原理如图 3 所示。

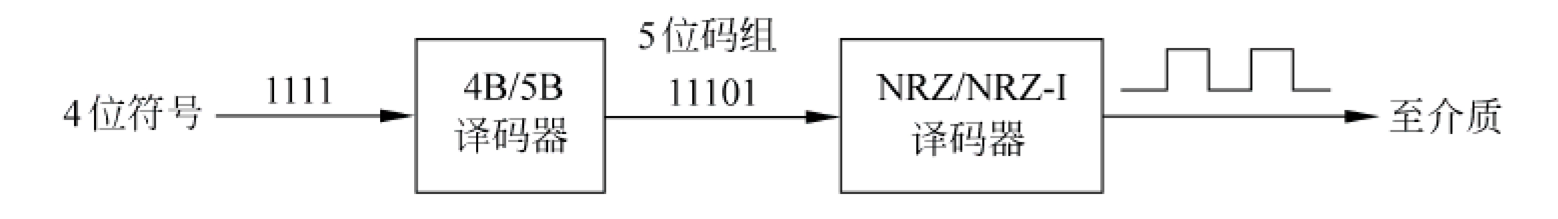


图 3 FDDI 编码

这是一种两级编码方案。基本的编码方法是“见 1 就翻不归零码”（NRZ-I）。NRZ-I 代码序列中 1 的个数越多，越能提供同步信息，但如果遇到长串的 0，则不能提供同步信息。所以在发送到传送介质去之前需经过一次 4B/5B 编码的变换，发送器扫描发送的比特序列，4 位分为一组，然后按照表 1 的对应规则变换成 5 位的代码。

表 1 4B/5B 编码规则

十六进制数	4 位二进制数	4B/5B 码	十六进制数	4 位二进制数	4B/5B 码
0	0000	11110	8	1000	10010
1	0001	01001	9	1001	10011
2	0010	10100	A	1010	10110
3	0011	10101	B	1011	10111
4	0100	01010	C	1100	11010
5	0101	01011	D	1101	11011
6	0110	01110	E	1110	11100
7	0111	01111	F	1111	11101

5 位二进制代码共有 32 种状态，在表 1 选用的 5 位代码中 1 的个数都不少于两个。这样就保证了在介质上传输的代码能够提供足够多的同步信息。

4B/5B 编码的效率为 4/5=80%，对于 100Mb/s 的数据速率，需要的波特率为 100M÷80%=125M 波特。

参考答案

（13）C

试题（14）

在以太网中使用 CRC 校验码，其生成多项式是＿（14）＿。

（14）A．$G(X)=X^{16}+X^{12}+X^{5}+1$

B．$G(X)=X^{16}+X^{15}+X^{2}+1$

C．$G(X)=X^{12}+X^{11}+X^{3}+X^{2}+X+1$

D．$G(X)=X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{3}+X+1$

试题（14）分析

为了能对不同的错误模式进行校验，已经研究出了几种 CRC 生成多项式的国际标准。

CRC-CCITT　$G(X)=X^{16}+X^{12}+X^{5}+1$

CRC-16　$G(X)=X^{16}+X^{15}+X^{2}+1$

CRC-12　$G(X)=X^{12}+X^{11}+X^{3}+X^{2}+X+1$

CRC-32　$G(X)=X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{2}+X+1$

其中 CRC-32 用在以太网中，这种生成多项式能产生 32 位的帧校验序列。

参考答案

（14）D

试题（15）

8 个 9600b/s 的信道按时分多路复用在一条线路上传输，在统计 TDM 情况下，假定每个子信道有 80%的时间忙，复用线路的控制开销为 5%，那么复用线路的带宽为＿（15）＿。

（15）A．32Kb/s　　B．64Kb/s　　C．72Kb/s　　D．96Kb/s

试题（15）分析

8 个 9600b/s 的信道复用在一条线路上，按照同步时分多路方式计算，复用线路的带宽为

$$9600\text{b/s}\times 8=76800\text{b/s}$$

在统计 TDM 情况下，每个子信道有 80%的时间忙，复用线路的控制开销为 5%，则复用线路的带宽为

$$76800\text{b/s}\times 80\%\times 105\%\approx 64\text{Kb/s}$$

参考答案

（15）B

试题（16）

设信道带宽为 4kHz，信噪比为 30dB，按照香农定理，信道的最大数据速率约等于__（16）__。

（16）A．10Kb/s　　B．20Kb/s　　C．30Kb/s　　D．40Kb/s

试题（16）分析

在有噪声信道中，香农（Shannon）定理计算出的信道容量为：

$$C = W\log_2(1+\frac{S}{N})$$

其中，W 为信道带宽，S 为信号的平均功率，N 为噪声平均功率，S/N 叫做信噪比。由于在实际使用中 S 与 N 的比值太大，故常取其分贝数（dB）。分贝与信噪比的关系为

$$\text{dB}=10\log_{10}\frac{S}{N}$$

例如当 S/N=1000 时，信噪比为 30dB。这个公式与信号取的离散值个数无关，也就是说无论用什么方式调制，只要给定了信噪比，则单位时间内最大的信息传输量就确定了。根据题意，信道带宽为 4 000Hz，信噪比为 30dB，则最大数据速率为

$$C=4\,000\log_2(1+1\,000)\approx 4\,000\times 9.97\approx 40\text{Kb/s}$$

参考答案

（16）D

试题（17）、（18）

在 E1 载波中，每个子信道的数据速率是__（17）__，E1 载波的控制开销占__（18）__。

（17）A．32Kb/s　　B．64Kb/s　　C．72Kb/s　　D．96Kb/s

（18）A．3.125%　　B．6.25%　　C．1.25%　　D．25%

试题（17）、（18）分析

CCITT 的 E1 载波提供 2.048 Mb/s 的数据传输速率。它把 32 个 8 位一组的数据样本组装成 125μs 的基本帧，其中 30 个子信道用于传送数据，两个子信道用于传送控制信令，每 4 帧能提供 64 个控制位。我国和欧洲使用 E1 作为数字载波的传输标准。在 E1 载波中，每个子信道的数据速率是

$$8\div 125\mu s=64\text{Kb/s}$$

E1 载波的控制开销为

$$2\div 32=6.25\%$$

参考答案

（17）B　（18）B

试题（19）

在 HFC 网络中，Cable Modem 的作用是__（19）__。

（19）A．用于调制解调和拨号上网
B．用于调制解调以及作为以太网卡接口
C．用于连接电话线和用户终端计算机
D．连接 ISDN 接口和用户终端计算机

试题（19）分析

电缆调制解调器（Cable Modem，CM）是基于 HFC 网络的宽带接入技术。CM 是用户设备与同轴电缆网络的接口。在下行方向，它接收前端设备 CMTS （Cable Modem Termination System）发送来的 QAM 信号，经解调后传送给 PC 的以太网接口。在上行方向，CM 把 PC 发送的以太帧封装在时隙中，经 QPSK 调制后，通过上行数据通路传送给 CMTS。

CM 不单纯是调制解调器，它集 MODEM、调谐器、加/解密设备、桥接器、网络接口卡、SNMP 代理和以太网集线器等功能于一身，无需拨号上网，不占用电话线路，可永久连接。大多数 Cable Modem 提供一个标准的 10Base-T 以太网接口，可以同用户的 PC 或局域网集线器相联。

参考答案

（19）B

试题（20）

以下属于对称数字用户线路（Symmetrical Digital Subscriber Line）的是 （20） 。

（20）A．HDSL　　B．ADSL　　C．RADSL　　D．VDSL

试题（20）分析

数字用户线路（Digital Subscriber Line，DSL）是基于普通电话线的宽带接入技术。它可以在一根铜线上分别传送数据和语音信号，其中数据信号并不通过电话交换设备，并且不需要拨号，属于专线上网方式。DSL 有许多模式，通常把所有的 DSL 技术统称为 xDSL，x 代表不同种类的 DSL 技术。

按数据传输的上、下行传输速率的相同和不同，DSL 有对称和非对称两种传输模式。对称 DSL 技术中，上、下行传输速率相同，主要有 HDSL、SDSL 等，用于替代传统的 T1/E1 接入技术。

高比特率用户数字线 HDSL 采用两对或三对双绞线提供全双工数据传输，支持 $n\times$64Kb/s（n=1，2，3，…）的各种速率，较高的速率可达 1.544Mb/s 或 2.048Mb/s，传输距离可达 3～5km，技术上比较成熟，在视频会议、远程教学和移动电话基站连接等方面得到了广泛应用。

SDSL（单线路用户数字线）在单一双绞线上支持多种对称速率的连接，用户可根据数据流量，选择最经济合适的速率。在 0.4mm 双绞线上的最大传输距离可达 3km 以上，能够支持诸如电视会议和协同计算等各种要求上、下行通信速率一致的应用。SDSL 标

准目前还处于发展中。

非对称 DSL 技术的上、下行传输速率不同，适用于对双向带宽要求不一样的应用，例如 Web 浏览、多媒体点播、信息发布等。

ADSL（Asymmetrical Digital Subscriber Line）是一种非对称 DSL 技术，在一对铜线上可提供上行速率 512Kb/s～1Mb/s，下行速率 1～8Mb/s，有效传输距离在 3～5km 左右。在进行数据传输的同时还可以使用第三个信道进行 4kHz 的语音传输。现在比较成熟的 ADSL 标准有 G.DMT 和 G.Lite 两种。G.DMT 是全速率的 ADSL 标准，支持 8Mb/s 的下行速率及 1.5Mb/s 的上行速率，但它要求用户端安装 POTS 分离器，比较复杂且价格昂贵；G.Lite 标准速率较低，下行速率为 1.5Mb/s，上行速率为 512Kb/s，但省去了 POTS 分离器，成本较低且便于安装。G.DMT 较适用于小型办公室（SOHO），而 G.Lite 则更适用于普通家庭。

RADSL（速率自适应用户数字线）支持同步和非同步传输方式，下行速率为 640Kb/s～12Mb/s，上行速率为 128Kb/s～1Mb/s，也支持数据和语音同时传输，具有速率自适应的特点。RADSL 可以根据双绞线的质量和传输距离动态调整用户的访问速度。RADSL 允许通信双方的 MODEM 寻找流量最小的频道来传送数据，以保证一定的数据速率。RADSL 特别适用于线路质量千差万别的农村、山区等地区使用。

VDSL（甚高比特率数字用户线）可在较短的距离上获得极高的传输速率，是各种 DSL 中速度最快的一种。在一对铜双绞线上，VDSL 的下行速率可以扩展到 52Mb/s，同时允许 1.5～2.3Mb/s 的上行速率，但传输距离只有 300～1000m。当下行速率降至 13Mb/s 时，传送距离可达到 1.5km 以上，此时上行速率为 1.6～2.3Mb/s 左右。传输距离的缩短，会使码间干扰大大减少，数字信号处理就大为简化，所以其设备成本要比 ADSL 低。

参考答案

（20）A

试题（21）

关于 ARP 表，以下描述中正确的是<u>（21）</u>。

（21）A．提供常用目标地址的快捷方式来减少网络流量

B．用于建立 IP 地址到 MAC 地址的映射

C．用于在各个子网之间进行路由选择

D．用于进行应用层信息的转换

试题（21）分析

ARP 协议的作用是由目标的 IP 地址发现对应的 MAC 地址。如果源站要和一个新的目标通信，首先由源站发出 ARP 请求广播包，其中包含目标的 IP 地址，然后目标返回 ARP 应答包，其中包含了自己的 MAC 地址。这时，源站一方面把目标的 MAC 地址装入要发送的数据帧中，一方面把得到的 MAC 地址添加到自己的 ARP 表中。当一个站与

多个目标进行了通信后，在其 ARP 表中就积累了多个表项，每一项都是 IP 地址与 MAC 地址的映射关系。ARP 表通常用于由 IP 地址查找对应的 MAC 地址。

参考答案

（21）B

试题（22）

因特网中的协议应该满足规定的层次关系，下面的选项中能正确表示协议层次和对应关系的是__（22）__。

（22）A.

SNMP	TFTP
UDP	TCP
IP	

B.

SNMP	HTTP
TCP	UDP
IP	

C.

HTTP	TFTP
TCP	UDP
IP	

D.

SMTP	TELNET
TCP	UDP
IP	

试题（22）分析

Internet 协议要满足一定的封装关系，上层协议封装在下层协议数据单元中传送。应用层协议 HTTP（超文本传输协议）通过 TCP 连接发送，SNMP（简单网络管理协议）利用 UDP 数据报传送，TFTP（简单文件传输协议）也是利用 UDP 数据报传送，而 TELNET（远程登录协议）则是建立在 TCP 连接之上。

参考答案

（22）C

试题（23）

BGP 协议的作用是__（23）__。

（23）A．用于自治系统之间的路由器间交换路由信息

B．用于自治系统内部的路由器间交换路由信息

C．用于主干网中路由器之间交换路由信息

D．用于园区网中路由器之间交换路由信息

试题（23）分析

边界网关协议（BGP）是一种外部网关协议（EGP），用于自治系统之间的路由器交换路由信息。OSPF 和 RIP 等属于内部网关协议（IGP），用于自治系统内部的路由器之间交换路由信息。Internet 主干网的路由器之间利用网关对网关的协议（Getway-to-Getway Protocol，GGP）交换路由信息，如图 4 所示。

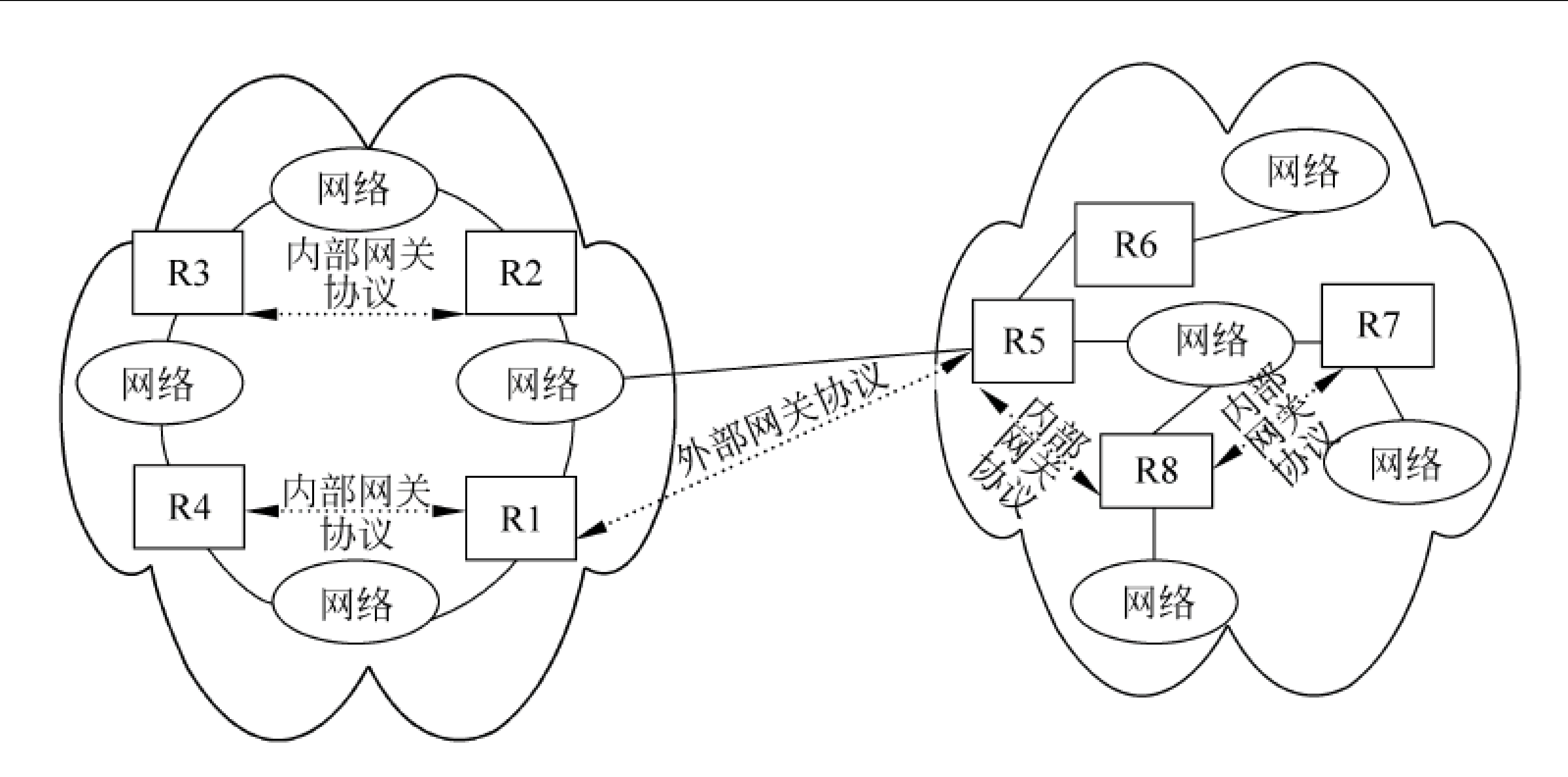


图 4 内部网关协议和外部网关协议

BGP 的主要功能是控制路由策略，例如是否愿意转发过路的分组等。BGP 的 4 种报文表示在表 2 中，这些报文通过 TCP 连接传送。BGP 用 4 种报文可实现以下三个功能过程。

表 2 BGP 的 4 种报文

报 文 类 型	功 能 描 述
建立（Open）	建立邻居关系
更新 Update	发送新的路由信息
保持活动状态（Keepalive）	对 Open 的应答/周期性地确认邻居关系
通告	报告检测到的错误

（1）建立邻居关系。位于不同自治系统中的两个路由器首先要建立邻居关系，然后才能周期性地交换路由信息。首先由一个路由器发送 Open 报文，另一个路由器若愿意接受请求则以 Keepalive 报文应答。Open 报文中包含发送者的 IP 地址及其所属自治系统的标识，另外还有一个保持时间参数。接收者把 Open 报文中的保持时间与自己的保持时间计数器比较，选取其中的较小者，这个数就是一次交换信息保持有效的最长时间。

（2）邻居可到达性。这个过程维护邻居关系的有效性。通过周期地互相发送 Keepalive 报文，双方都知道对方的活动状态。

（3）网络可到达性。每个路由器保持一个数据库，记录着可到达的所有网络。当情况变化时用 Update 报文把最新信息及时地广播给所有实现 BGP 的路由器。Update 报文包含两类信息：一类是发布过的、而现在要取消的路由器的表，另一类是新路由的属性信息。前者列出了已经关机或失效的一些路由器，接收者应将其从本地数据库中删除。后者包含以下三种信息。

① 网络层可到达信息（NLRI）：发送路由器可到达的网络的列表。

② 通过的自治系统（AS_Path）：是数据报经过的自治系统的标识符，这主要用于通信策略控制。例如机密报文可能要选择某些自治系统，或者根据某个自治系统的性能、拥挤程度等参数，从而决定绕开该网络。

③ 下一跳（Next-Hop）：指可作为下一步转发的边界路由器的 IP 地址。可以是发送者自己的地址，也可以是另外的边界路由器的地址。例如在图 3 中，R1 告诉 R5，通过 R2 也可以到达 AS1。虽然 R2 没有实现 BGP，也没有和 R5 建立邻居关系，但是 R1 通过 IGP 知道了与 R2 有关的信息。

参考答案

（23）A

试题（24）

关于 RIP，以下选项中错误的是__（24）__。

（24）A．RIP 使用距离矢量算法计算最佳路由

B．RIP 规定的最大跳数为 16

C．RIP 默认的路由更新周期为 30 秒

D．RIP 是一种内部网关协议

试题（24）分析

RIP 的原型最早出现在 UNIX Berkley 4.3 BSD 中，它使用了 Bellman-Ford 的距离矢量路由算法，用于在早期的 ARPANET 中计算最佳路由。现在的 RIP，作为内部网关协议运行在基于 TCP/IP 的网络中。RIP 适用于小型网络，因为它允许的跳步数不超过 15 步。

RIP 分为两个版本，RIPv1（RFC 1058，1988）是早期的路由协议，现在仍然广泛使用。RIPv1 使用目标地址为 255.255.255.255 的本地广播来共享路由信息，默认的路由更新周期为 30s，持有时间（Hold-Down Time）为 180s。也就是说，RIP 路由器每 30s 向它的所有邻居发送一次路由更新报文；如果在 180s 之内没有从某个邻居接收到路由更新报文，则认为该邻居已经崩溃或者其间的连接已失效。这时如果从其他邻居收到了有关同一目标的路由更新报文，则用新的路由信息替换已失效的路由表项，否则对应的路由表项被删除。

RIP 以跳步计数（hop count）来度量路由费用，显然这不是最好的度量标准。例如，若有两条到达某个网络的连接，一个连接是经过两跳的 10MB 以太网连接，一个连接是经过一跳的 64K WAN 连接，则 RIP 选取 WAN 连接作为最佳路由。在 RIP 协议中，15 跳是最大的跳数，16 跳就是不可到达网络，经过 16 跳的任何分组将被路由器丢弃。

RIPv1 是有类别的协议（classful protocol），这意味着配置 RIPv1 时必须给定 A、B 或 C 类 IP 地址和子网掩码，例如不能把子网掩码 255.255.255.0 用于 B 类网络 172.16.0.0。

对于同一个目标，RIP 路由表项中最多可以有 6 条等费用的通路，虽然默认的是 4 条。RIP 可以实现等费用通路的负载均衡（equal-cost load balancing），这种机制提供了

链路冗余，以对付可能出现的连接失效，但是 RIP 不支持不等费用通路的负载均衡，这种功能出现在 IGRP 和 EIGRP 中。

RIPv2 是增强了的 RIP 协议，定义在 RFC 1721 和 RFC 1722（1994）两个文件中。RIPv2 基本上还是一个距离矢量路由协议，但是有三方面的改进。首先，它使用组播而不是广播来传播路由更新报文，并且采用了触发更新（triggered update）机制来加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次，RIPv2 是一个无类别的协议（classless protocol），可以使用可变长子网掩码（VLSM），也支持无类别域间路由（CIDR），这些功能使得网络的设计更具有伸缩性。第三个增强是 RIPv2 支持认证，使用经过散列的口令字来限制更新信息的传播。其他方面的特性与第一版相同，例如以跳步计数来度量路由费用，允许的最大跳步数为 15 等。

参考答案

（24）B

试题（25）

路由汇聚（Route Summarization）是把小的子网汇聚成大的网络，下面 4 个子网：172.16.193.0/24、172.16.194.0/24、172.16.196.0/24 和 172.16.198.0/24，进行路由汇聚后的网络地址是<u>（25）</u>。

（25）A．172.16.192.0/21　　B．172.16.192.0/22
　　　C．172.16.200.0/22　　D．172.16.224.0/20

试题（25）分析

网络 172.16.193.0/24 的二进制表示为：　10101100 00010000 11000001 00000000
网络 172.16.194.0/24 的二进制表示为：　10101100 00010000 11000010 00000000
网络 172.16.196.0/24 的二进制表示为：　10101100 00010000 11000100 00000000
网络 172.16.198.0/24 的二进制表示为：　10101100 00010000 11000110 00000000

可以看出，按照最长匹配规则，得到的网络地址为：

172.16.192.0/21　10101100 00010000 11000000 00000000

参考答案

（25）A

试题（26）

分配给某校园网的地址块是 202.105.192.0/18，该校园网包含<u>（26）</u>个 C 类网络。

（26）A．6　　B．14　　C．30　　D．62

试题（26）分析

网络 202.105.192.0/18 的二进制表示为：　11001010 01101001 11000000 00000000

这其中包含 62 个 C 类网络。

参考答案

（26）D

试题（27）

以下地址中属于 D 类地址的是__（27）__。

（27）A．224. 116. 213. 0　　B．110. 105. 207. 0
　　C．10. 105. 205. 0　　D．192. 168. 0. 7

试题（27）分析

D 类网络地址的首字节是 11100000，即 224，所以 224. 116. 213. 0 为 D 类组播地址。

参考答案

（27）A

试题（28）

在 Windows 操作系统中，采用__（28）__命令来测试到达目标所经过的路由器数目及 IP 地址。

（28）A．ping　　B．tracert　　C．arp　　D．nslookup

试题（28）分析

ping 是 Windows 系列自带的一个可执行命令，用于验证与远程计算机的连接。该命令只有在安装了 TCP/IP 协议后才可以使用。ping 命令的主要作用是通过发送数据包并接收应答信息来检测两台计算机之间的网络是否连通。当网络出现故障的时候，可以用这个命令来预测故障和确定故障地点。ping 命令成功只是说明当前主机与目的主机之间存在一条连通的路径。如果不成功，则考虑网线是否连通、网卡设置是否正确、IP 地址是否可用等。利用它可以检查网络是否能够连通。ping 命令应用格式：ping IP 地址。该命令还可以加参数使用，输入 ping 按回车键即可看到详细说明。ping 命令的应用如下图所示。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\yantihua>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\yantihua>_
```

tracert 命令主要用来显示数据包到达目的主机所经过的路径。该命令的使用格式是在 DoS 命令提示符下或者直接在运行对话框中输入如下命令：tracert 主机 IP 地址或主机名。执行结果返回数据包到达目的主机前所经历的中继站清单，并显示到达每个中继站

的时间。该功能同 ping 命令类似，但它所看到的信息要比 ping 命令详细得多，它把用户送出的到某一站点的请求包，所走的全部路由都告诉用户，并且告诉用户通过该路由的 IP 是多少，通过该 IP 的时延是多少。具体的 tracert 命令后还可跟参数，输入 tracert 后按回车键，其中会有很详细的说明。tracert 命令的应用如下图所示。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\yantihua>tracert www.sina.com.cn

Tracing route to jupiter.sina.com.cn [202.205.3.143]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2    <1 ms    <1 ms    <1 ms  202.117.115.254
  3    10 ms    10 ms    12 ms  210.27.15.9
  4     1 ms     1 ms     1 ms  202.200.29.141
  5     1 ms     1 ms     1 ms  202.200.29.9
  6    <1 ms    <1 ms    <1 ms  202.200.29.5
  7     1 ms     1 ms     1 ms  202.112.53.141
  8    78 ms     *        *     202.112.36.213
  9    67 ms    67 ms    67 ms  cd1.cernet.net [202.112.53.74]
 10    79 ms    72 ms    71 ms  wdc1.cernet.net [202.112.38.82]
 11    67 ms    68 ms    70 ms  202.205.13.249
 12    73 ms    72 ms    71 ms  202.205.13.210
 13    77 ms    76 ms    78 ms  202.205.3.143

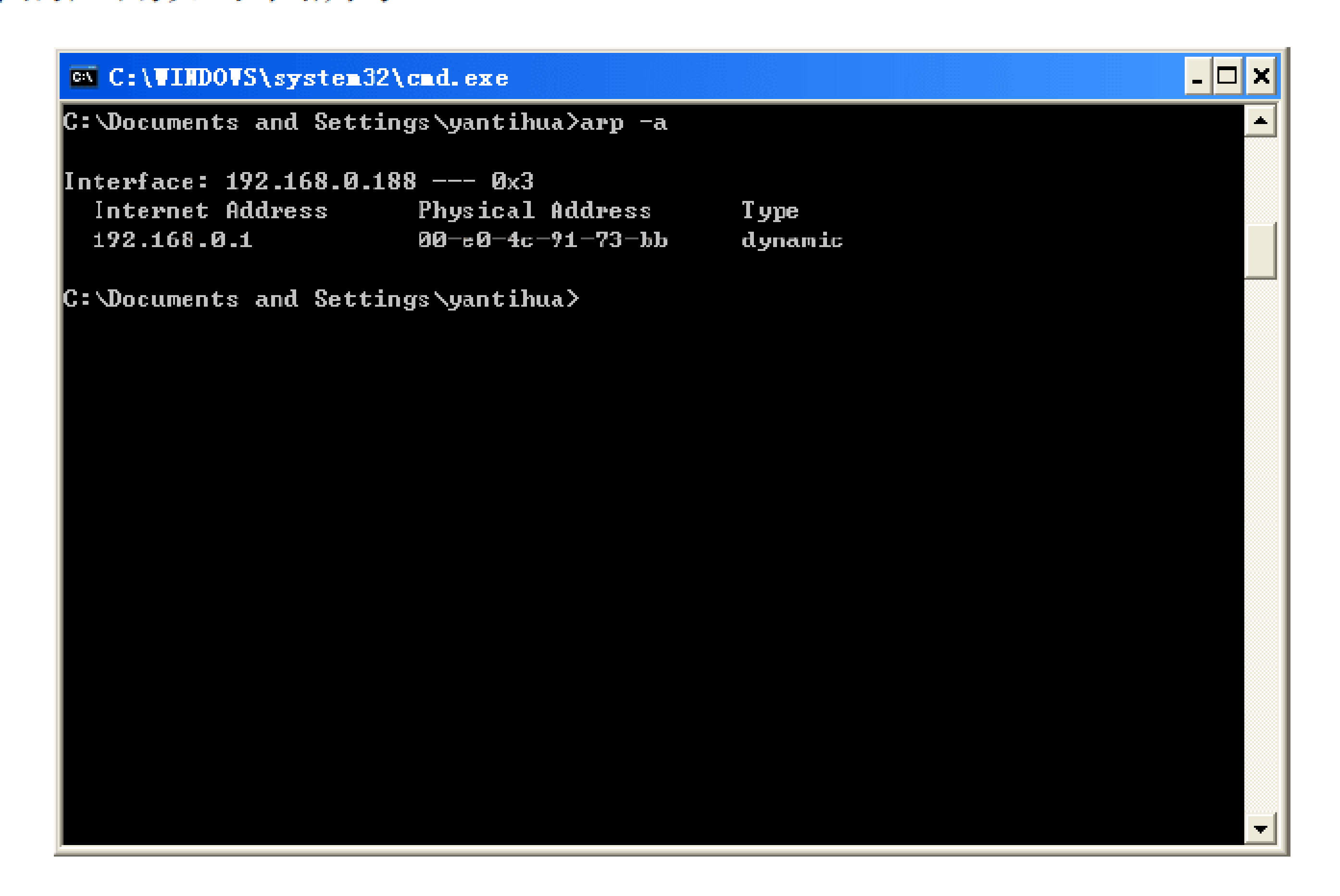
Trace complete.

C:\Documents and Settings\yantihua>
```

arp 命令用以显示和修改“地址解析协议（ARP）”缓存中的项目。ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。如果在没有参数的情况下使用，则 arp 命令将显示帮助信息。语法如下：

```
arp[-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d
InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]
```

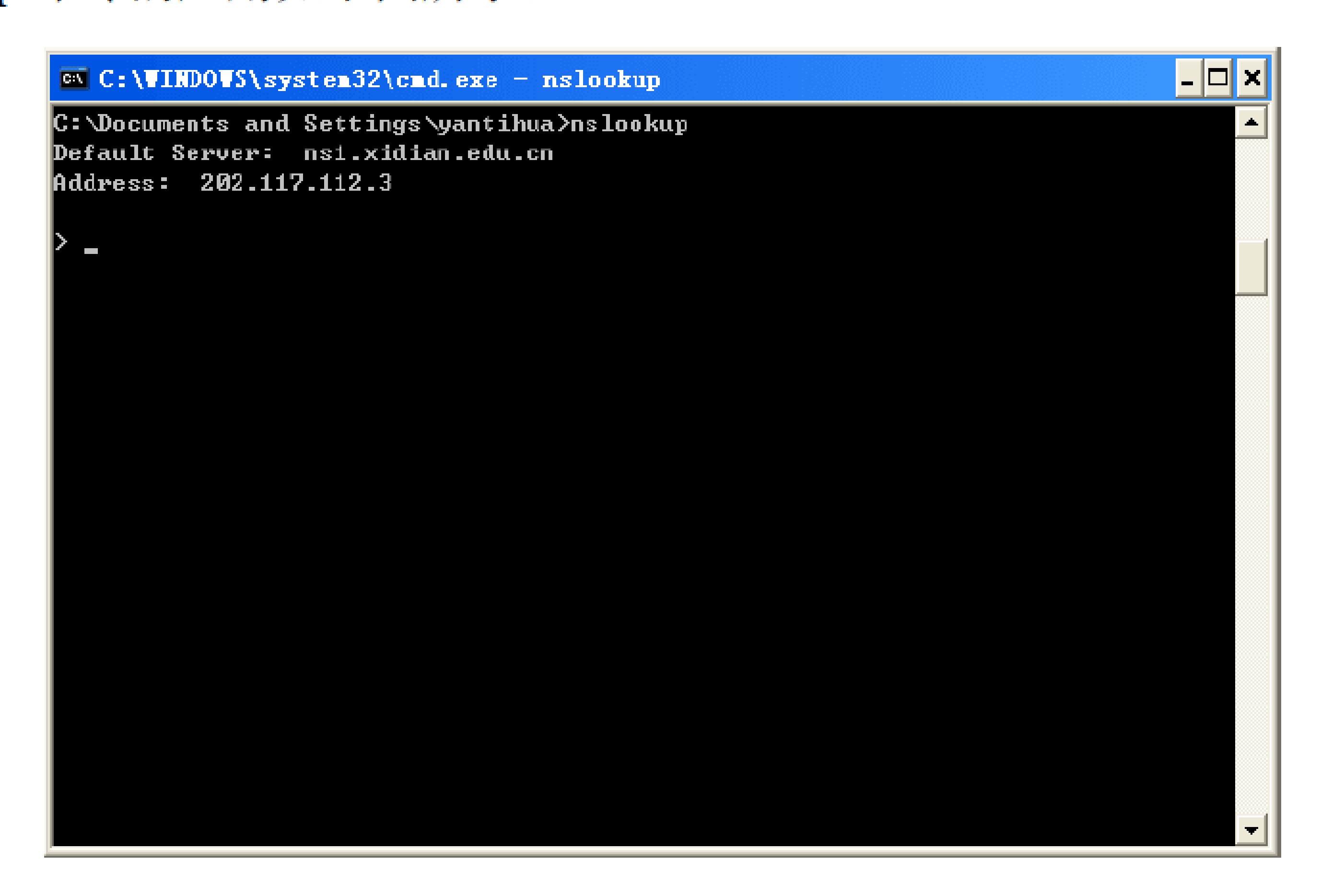
arp 命令的应用如下图所示。



nslookup 命令的功能是查询一台机器的 IP 地址和其对应的域名。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的 IP 地址对应的域名。

该命令的一般格式为：nslookup [IP 地址/域名]

nslookup 命令的应用如下图所示。



参考答案

（28）B

试题（29）、（30）

FTP 使用的传输层协议为__（29）__；FTP 默认的控制端口号为__（30）__。

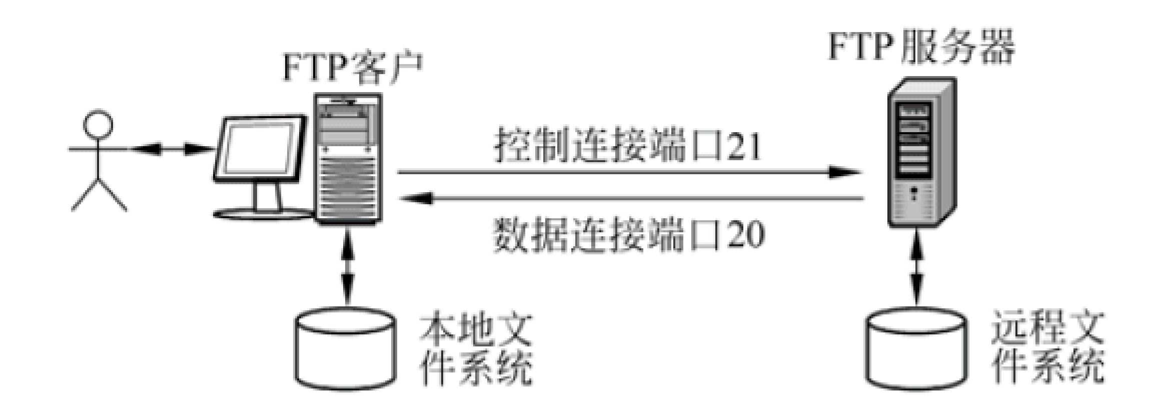
（29）A．HTTP　　B．IP　　C．TCP　　D．UDP

（30）A．80　　B．25　　C．20　　D．21

试题（29）、（30）分析

FTP（File Transfer Protocol）即文件传输协议，是因特网上的另一项主要服务，这项服务的名字是由该服务使用的协议引申而来的，各类文件存放于 FTP 服务器，可以通过 FTP 客户程序连接 FTP 服务器，然后利用 FTP 协议进行文件的“下载”或“上传”。

FTP 使用的传输层协议为 TCP，通常有两个端口，一个用作控制连接，一个用作数据传输。默认情况下，端口 21 用作控制连接，端口 20 用作数据传输，如下图所示。



参考答案

（29）C　（30）D

试题（31）

在 Linux 操作系统中，（31） 文件负责配置 DNS，它包含了主机的域名搜索顺序和 DNS 服务器的地址。

（31）A．/etc/hostname　　B．/etc/host.conf

C．/etc/resolv.conf　　D．/etc/name.conf

试题（31）分析

在 Linux 操作系统中，/etc/hostname 文件包含了 Linux 系统的主机名称，包括完全的域名；/etc/host.conf 文件指定如何解析主机域名，Linux 通过解析库来获得主机名对应的 IP 地址；/etc/resolv.conf 文件负责配置 DNS，它包含了主机的域名搜索顺序和 DNS 服务器的地址。

参考答案

（31）C

试题（32）

Linux 系统在默认情况下将创建的普通文件的权限设置为 （32） 。

（32）A．-rw-r-r-　　B．-r-r-r-

C．-rw-rw-rwx-　　D．-rwxrwxrw-

试题（32）分析

Linux 系统对文件的访问设定了三级权限：文件所有者，文件所有者同组的用户，其他用户；同时对文件的访问做三种处理操作：读取、写入和执行。Linux 文件被创建时，文件所有者可以对该文件的权限进行设置。默认情况下，系统将创建的普通文件的权限设置为-rw-r-r-。

参考答案

（32）A

试题（33）

在 Linux 系统中，用户组加密后的口令存储在 （33） 文件中。

（33）A．/etc/passwd　　B．/etc/shadow

C．/etc/group　　D．/etc/shells

试题（33）分析

/etc/passwd 文件是 Linux 系统中用于用户管理的重要文件，这个文件对所有用户都是可读的，Linux 系统中的每个用户在/etc/passwd 文件中都有一行对应的记录，用户在登录时，会先在/etc/passwd 文件中找到用户 ID。/etc/shadow 保存着加密后的用户口令。而/etc/group 是管理用户组的基本文件，在/etc/group 中每行记录对应一个组，它包括用户组名，加密后的组口令，组 ID 和组成员列表。

参考答案

（33）C

试题（34）

以下关于 Windows Server 2003 的域管理模式的描述中，正确的是__（34）__。

（34）A．域间信任关系只能是单向信任

B．只有一个主域控制器，其他都为备份域控制器

C．每个域控制器都可以改变目录信息，并把变化的信息复制到其他域控制器

D．只有一个域控制器可以改变目录信息

试题（34）分析

Windows Server 2003 采用了活动目录技术，域间信任关系有多种形式，在 Windows Server 2003 中采用了多主机复制模式，多个域控制器没有主次之分。域中每个域控制器即可接受其他域控制器的变化信息而改变目录信息，也可把变化的信息复制到其他域控制器。

参考答案

（34）C

试题（35）

在 Windows Server 2003 中，默认情况下__（35）__组用户拥有访问和完全控制终端服务器的权限。

（35）A．Interactive　　B．Network　　C．Everyone　　D．System

试题（35）分析

Windows Server 2003 在系统安装完毕后，会自动建立几个特殊组，其中包括 Interactive（任何在本机登录的用户）、Network（任何通过网络连接的用户）、Everyone（任何使用计算机的人员）和 System（系统组）等。而终端服务可以让操作者通过远程访问服务器桌面。默认情况下，只有系统管理员组（Administrators）和系统组用户（System）拥有访问和完全控制终端服务器的权限。

参考答案

（35）D

试题（36）

以下关于 DHCP 服务的说法中正确的是__（36）__。

（36）A．在一个子网内只能设置一台 DHCP 服务器，以防止冲突

B．在默认情况下，客户机采用最先到达的 DHCP 服务器分配的 IP 地址

C．使用 DHCP 服务，无法保证某台计算机使用固定 IP 地址

D．客户端在配置时必须指明 DHCP 服务器 IP 地址，才能获得 DHCP 服务

试题（36）分析

DHCP 就是 Dynamic Host Configuration Protocol（动态主机配置协议）的缩写，当

DHCP 客户机首次启动时，客户机向 DHCP 服务器发送一个 Dhcpdiscover 数据包，该数据包表达了客户机的 IP 租用请示，在大多数情况下，客户机接受收到的第一个 dhcpoffer。使用 DHCP 服务时，可以通过保留 IP 与 MAC 地址保证某台计算机使用固定 IP 地址。客户端在配置时不必指明 DHCP 服务器 IP 地址，就能获得 DHCP 服务。

参考答案

（36）B

试题（37）

使用代理服务器（Proxy Server）访问 Internet 的主要功能不包括__（37）__。

（37）A．突破对某些网站的访问限制

B．提高访问某些网站的速度

C．避免来自 Internet 上病毒的入侵

D．隐藏本地主机的 IP 地址

试题（37）分析

代理服务器是介于浏览器和 Web 服务器之间的一台服务器，当用户通过代理服务器上网浏览时，浏览器不是直接到 Web 服务器去取回网页而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息并传送到用户的浏览器。使用代理服务器访问 Internet 时可以突破对某些网站的访问限制、提高访问某些网站的速度、隐藏本地主机的 IP 地址，但是不能避免来自 Internet 上病毒的入侵。

参考答案

（37）C

试题（38）、（39）

POP3 协议采用__（38）__模式，当客户机需要服务时，客户端软件（Outlook Express 或 FoxMail）与 POP3 服务器建立__（39）__连接。

（38）A．Browser/Server　　B．Client/Server

C．Peer to Peer　　D．Peer to Server

（39）A．TCP　　B．UDP　　C．PHP　　D．IP

试题（38）、（39）分析

POP3 协议采用 Client/Server 模式，当客户机需要服务时，客户端软件（Outlook Express 或 FoxMail）与 POP3 服务器建立 TCP 连接。

参考答案

（38）B　（39）A

试题（40）

DES 是一种__（40）__算法。

（40）A．共享密钥　　B．公开密钥　　C．报文摘要　　D．访问控制

试题（40）分析

DES（Data Encryption Standard）是美国政府 1977 年采用的加密标准，最初是由 IBM 公司在 70 年代初期开发的。美国政府在 1981 年又将 DES 进一步规定为 ANSI 标准。

DES 是一个对称密钥系统，加密和解密使用相同的密钥。它通常选取一个 64 位（bit）的数据块，使用 56 位的密钥，在内部实现多次替换和变位操作来达到加密的目的。

参考答案

（40）　A

试题（41）

在 Linux 系统中，利用__（41）__命令可以分页显示文件的内容。

（41）A．list　　B．cat　　C．more　　D．cp

试题（41）分析

在 Linux 系统中，cat 命令用来在屏幕上滚动显示文件内容；more 命令可以分页显示文件内容；cp 为文件复制命令。

参考答案

（41）C

试题（42）

在 Windows 操作系统中，要实现一台具有多个域名的 Web 服务器，正确的方法是__（42）__。

（42）A．使用虚拟目录　　B．使用虚拟主机

C．安装多套 IIS　　D．为 IIS 配置多个 Web 服务端口

试题（42）分析

在 Windows 操作系统中，Web 服务器只能安装一套 IIS 系统，使用虚拟目录和多个 Web 服务端口可以实现多个网站的发布，但是其域名是相同的，而使用虚拟主机可以实现一台具有多个域名的 Web 服务器。

参考答案

（42）B

试题（43）

下列行为不属于网络攻击的是__（43）__。

（43）A．连续不停 Ping 某台主机　　B．发送带病毒和木马的电子邮件

C．向多个邮箱群发一封电子邮件　　D．暴力破解服务器密码

试题（43）分析

网络攻击是以网络为手段窃取网络上其他计算机的资源或特权，对其安全性或可用性进行破坏的行为。网络攻击又可分为主动攻击和被动攻击。被动攻击就是网络窃听，截取数据包并进行分析，从中窃取重要的敏感信息。被动攻击很难被发现，因此预防很重要，防止被动攻击的主要手段是数据加密传输。为了保护网络资源免受威胁和攻击，

在密码学及安全协议的基础上发展了网络安全体系中的5类安全服务，它们是：身份认证、访问控制、数据保密、数据完整性和不可否认。对这5类安全服务，国际标准化组织ISO已经有了明确的定义。主动攻击包括窃取、篡改、假冒和破坏。字典式口令猜测，IP 地址欺骗和服务拒绝攻击等都属于主动攻击。一个好的身份认证系统（包括数据加密、数据完整性校验、数字签名和访问控制等安全机制）可以用于防范主动攻击，但要想杜绝主动攻击很困难，因此对付主动攻击的另一措施是及时发现并及时恢复所造成的破坏，现在有很多实用的攻击检测工具。

常用的有以下9种网络攻击方法。

1．获取口令。
2．放置特洛伊木马程序。
3．WWW的欺骗技术。
4．电子邮件攻击。
5．通过一个节点来攻击其他节点。
6．网络监听。
7．寻找系统漏洞。
8．利用账号进行攻击。
9．偷取特权。

参考答案

（43）C

试题（44）

采用Kerberos系统进行认证时，可以在报文中加入＿（44）＿来防止重放攻击。

（44）A．会话密钥　　B．时间戳　　C．用户ID　　D．私有密钥

试题（44）分析

Kerberos认证是一种使用对称密钥加密算法来实现通过可信第三方密钥分发中心的身份认证系统。客户方需要向服务器方递交自己的凭据来证明自己的身份，该凭据是由KDC专门为客户和服务器方在某一阶段内通信而生成的。凭据中包括客户和服务器方的身份信息和在下一阶段双方使用的临时加密密钥，还有证明客户方拥有会话密钥的身份认证者信息。身份认证信息的作用是防止攻击者在将来将同样的凭据再次使用。时间标记是检测重放攻击。

参考答案

（44）B

试题（45）

包过滤防火墙通过＿（45）＿来确定数据包是否能通过。

（45）A．路由表　　B．ARP表　　C．NAT表　　D．过滤规则

试题（45）分析

包过滤型防火墙工作在 OSI 网络参考模型的网络层和传输层，它根据数据包头源地址，目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用，是因为它不是针对各个具体的网络服务采取特殊的处理方式，适用于所有网络服务；之所以廉价，是因为大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的；之所以有效，是因为它在很大程度上满足了绝大多数企业的安全要求。

在整个防火墙技术的发展过程中，包过滤技术出现了两种不同的版本，称为“第一代静态包过滤”和“第二代动态包过滤”。

第一代静态包过滤类型防火墙

这类防火墙几乎是与路由器同时产生的，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括 IP 源地址、IP 目标地址、传输协议（如 TCP、UDP 和 ICMP 等）、TCP/UDP 目标端口和 ICMP 消息类型等。

第二代动态包过滤类型防火墙

这类防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为包状态监测（Stateful Inspection）技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目。

包过滤方式的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。但其弱点也是明显的：过滤判别的依据只是网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大地影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC（远程过程调用）一类的协议。另外，大多数过滤器中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证，很容易受到“地址欺骗型”攻击。对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常是和应用网关配合使用，共同组成防火墙系统。

参考答案

（45）D

试题（46）

目前在网络上流行的“熊猫烧香”病毒属于 （46） 类型的病毒。

（46）A．目录　　B．引导区　　C．蠕虫　　D．DOS

试题（46）分析

熊猫烧香是一种感染型的蠕虫病毒，它能感染系统中 exe、com、pif、src、html 和

asp 等文件，还能中止大量的反病毒软件进程并且会删除扩展名为 gho 的文件，该文件是系统备份工具 GHOST 的备份文件，使用户的系统备份文件丢失。

被感染的用户系统中所有.exe 可执行文件全部被改成熊猫举着三根香的模样。

参考答案

（46）C

试题（47）

多形病毒指的是__（47）__的计算机病毒。

（47）A．可在反病毒检测时隐藏自己　　B．每次感染都会改变自己

C．可以通过不同的渠道进行传播　　D．可以根据不同环境造成不同破坏

试题（47）分析

多形病毒是一种较为高级的病毒，这种病毒在每次感染后会改变自己。

参考答案

（47）B

试题（48）

SNMP 采用 UDP 提供数据报服务，这是由于__（48）__。

（48）A．UDP 比 TCP 更加可靠

B．UDP 数据报文可以比 TCP 数据报文大

C．UDP 是面向连接的传输方式

D．采用 UDP 实现网络管理不会太多增加网络负载

试题（48）分析

SNMP 定义为依赖于 UDP 数据报服务的应用层协议。SNMP 实体向管理应用程序提供服务，它的作用是把管理应用程序的服务调用变成对应的 SNMP 协议数据单元，并利用 UDP 数据报发送出去。之所以选择 UDP 协议而不是 TCP 协议，是因为 UDP 效率较高，这样实现网络管理不会太多地增加网络负载。但由于 UDP 不可靠，所以 SNMP 报文容易丢失。为此，对 SNMP 实现是将每个管理信息装配成单独的数据报独立发送，而且报文较短，不超过 484 个字节。

参考答案

（48）D

试题（49）

在 SNMPv2 中，一个实体发送一个报文一般经过四个步骤：

（1）加入版本号和团体名，构造报文；

（2）把 PDU、源和目标端口地址以及团体名传送给认证服务，认证服务产生认证码或对数据进行加密，返回结果；

（3）根据要实现的协议操作构造 PDU；

（4）进行 BER 编码，产生 0/1 比特串，发送出去。

这四个步骤的正确次序是__（49）__。

（49）A．（1）（3）（2）（4）　　B．（3）（2）（1）（4）
　　C．（4）（1）（3）（2）　　D．（2）（1）（3）（4）

试题（49）分析

在 SNMP v2 中，一个实体发送一个报文一般要经过下面 4 个步骤。

（1）根据要实现的协议操作构造 PDU；

（2）把 PDU、源和目标端口地址以及团体名传送给认证服务，认证服务产生认证码或对数据进行加密，返回结果；

（3）加入版本号和团体名，构造报文；

（4）进行 BER 编码，产生 0/1 比特串，发送出去。

参考答案

（49）B

试题（50）

嗅探器可以使网络接口处于杂收模式，在这种模式下，网络接口__（50）__。

（50）A．只能够响应与本地网络接口硬件地址相匹配的数据帧
　　B．只能够响应本网段的广播数据帧
　　C．只能响应组播信息
　　D．能够响应流经网络接口的所有数据帧

试题（50）分析

在一般情况下，网络上所有的计算机都可以接收到通过的数据帧，但对不属于自己的报文则不予响应，但是如果某工作站的网络接口处于杂收模式，那么它就可以捕获网络上所有的报文和帧，如果一个工作站被配置成这样的方式，它就是一个嗅探器。

参考答案

（50）D

试题（51）

把 IP 网络划分成子网，这样做的好处是__（51）__。

（51）A．增加冲突域的大小　　B．增加主机的数量
　　C．减小广播域的大小　　D．增加网络的数量

试题（51）分析

每一个网络是一个广播域，把 IP 网络划分成子网的好处是减少了广播域的大小。

参考答案

（51）C

试题（52）、（53）

局域网中某主机的 IP 地址为 172.16.1.12/20，该局域网的子网掩码为__（52）__，最多可以连接的主机数为__（53）__。

（52）A．255.255.255.0　　B．255.255.254.0
　　C．255.255.252.0　　D．255.255.240.0

（53）A．4094　　B．2044　　C．1024　　D．512

试题（52）、（53）分析

网络 172.16.1.12/20 的子网掩码为 11111111 11111111 11110000 00000000，即 255.255.240.0，其中的主机地址为 12 位，即 2^{12}–2=4094 个主机地址。

参考答案

（52）D　（53）A

试题（54）

下面的地址中，属于私网地址的是＿（54）＿。

（54）A．192.118.10.1　　B．127.1.0.1
　　C．172.14.2.240　　D．172.17.20.196

试题（54）分析

属于私网的 IP 地址为：1 个 A 类网络 10.0.0.0，16 个 B 类网络 172.15.0.0～172.31.0.0，256 个 C 类网络 192.168.0.0～192.168.255.0

参考答案

（54）D

试题（55）

一个主机的 IP 地址是 172.16.2.12/24，该主机所属的网络地址是＿（55）＿。

（55）A．172.0.0.0　　B．172.16.0.0　　C．172.16.2.0　　D．172.16.1.0

试题（55）分析

地址 172.16.2.12/24 的二进制表示为 10101100 00010000 00000010 00001100，子网掩码为 24 位，所以网络地址部分为 10101100 00010000 00000010 00000000，即 172.16.2.0。

参考答案

（55）C

试题（56）

配置路由器端口，应该在哪种提示符下进行？＿（56）＿

（56）A．R1 (config)#　　B．R1 (config-in)#
　　C．R1 (config-intf)#　　D．R1 (config-if)#

试题（56）分析

路由器的命令状态分为：

1．R1>

路由器处于用户命令状态，这时用户可以查看路由器的连接状态，访问其他网络和主机，但不能更改路由器配置的内容。

2．R1#

在“>”提示符下输入 enable，路由器进入特权命令状态，这时不但可以执行所有的用户命令，还可以看到和更改路由器的配置内容。

3．R1 (config)#

在“#”提示符下输入 configure terminal，这时路由器处于全局配置状态，可以配置路由器的全局参数。

4．R1 (config-if)#：端口配置状态。

R1 (config-line)#：线路配置状态。

R1 (config-router)#：路由协议配置状态。

在全局配置状态下，

输入 interface *type number.subinterface*，进入端口配置状态。

输入 line *type slot/number*，进入线路配置状态。

输入 router *protocol*，进入路由协议配置状态。

在路由器处于局部配置状态下，可以配置路由器的局部参数。

5．>

在开机后 60s 内按 ctrl-break 键，路由器进入 RXBOOT 状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导。

参考答案

（56）D

试题（57）

__（57）__能够显示路由器配置了哪种路由协议。

（57）A．R1 (config)# show ip route　　B．R1 > show ip route

C．R1 >show ip protocol　　D．R1 (config-if)# show ip protocol

试题（57）分析

在用户命令或特权命令状态下，show ip route 命令显示路由信息。

在用户命令或特权命令状态下，show ip protocol 命令显示配置的路由协议。

参考答案

（57）C

试题（58）

某端口的 IP 地址为 172.16.7.131/26，则该 IP 地址所在网络的广播地址是__（58）__。

（58）A．172.16.7.255　　B．172.16.7.129

C．172.16.7.191　　D．172.16.7.252

试题（58）分析

地址 172.16.7.131/26 的二进制表示是 10101100 00010000 00000111 10000011。

其广播地址是 10101100 00010000 00000111 10111111。

对应的十进制表示是 172.16.7.191。

参考答案

（58）C

试题（59）

当数据在两个 VLAN 之间传输时需要哪种设备?__（59）__

（59）A．二层交换机　B．网桥　C．路由器　D．中继器

试题（59）分析

当数据在两个 VLAN 之间传输时需要通过路由器或三层交换机。因为每个 VLAN 是一个广播域，在两个广播域之间进行数据交换需要第三层设备的支持。

参考答案

（59）C

试题（60）

在生成树协议（STP）中，根交换机是根据什么来选择的?__（60）__

（60）A．最小的 MAC 地址　B．最大的 MAC 地址
C．最小的交换机 ID　D．最大的交换机 ID

试题（60）分析

IEEE 802.1D 定义的生成树协议（Spanning Tree Protocol，STP）是一种链路管理协议，它在以太网中提供冗余链路以防止网络失效，而且能删除网络中的环路，使得任意两个工作站之间只存在一条活动链路。

STP 协议可以在复杂的以太网连接中选择一个生成树来消除环路，生成树的产生过程对上层协议是透明的。STP 利用网桥协议数据单元(Bridge Protocol Data Units ，BPDU）来交换状态信息，根据网桥标识来选择根网桥（或根交换机）和根端口，并为每个网段选择指定端口。网桥协议数据单元的格式如图 5 所示，其中各字段解释如下。

Protocol ID (2)	Version (1)	Type (1)	Flags (1)	Rood ID (8)	Root Path (4)
Sender BID (8)	Port ID (2)	M-Age (2)	Max Age (2)	Hello (2)	FD (2 Bytes)

图 5　BPDU 的格式

- ProtocolID：恒为 0。
- Version：恒为 0。
- Type：有两种类型的 BPDU，配置 BPDU 和 TCN PBDU。
- Flags：用于处理拓扑结构的改变。
- Root ID：网桥标识分为优先级和 MAC 地址两部分，标识最小的网桥成为根网桥。
- Root Path：根通路的费用。

- SenderBID：生成当前 BPDU 的网桥或交换机的 ID。
- Port ID：端口 ID，端口 1/1 的 ID 为 0x8001，端口 1/2 的 ID 为 0x8002。
- M-Age：报文发送的时间。
- Max Age：BPDU 保存的最长时间。
- Hello：配置周期间隔。
- FD：用于监听和学习状态的时间。

参考答案

（60）C

试题（61）

下面的交换机命令中哪一条为 2950 交换机端口指定 VLAN？__（61）__

（61）A．S1(config-if)# vlan-membership static

B．S1(config-if)# vlan database

C．S1(config-if)# switchport mode access

D．S1(config-if)# switchport access vlan 1

试题（61）分析

这 4 条命令解释如下。

- S1(config-if)# vlan-membership static *vlan_#*：该命令为 Cisco 1900 交换机端口分配 VLAN，后面必须说明端口号。
- S1(config-if)# vlan database：该命令用于 Cisco 2950 交换机，从特权模式进入 VLAN 配置模式。
- S1(config-if)# switchport mode access：将端口设置为接入链路连接。
- S1(config-if)# switchport access vlan 1：该命令用于 Cisco 2950 交换机，把当前端口分配给 VLAN1。

参考答案

（61）D

试题（62）

在以太网协议中使用 1-坚持型监听算法的特点是__（62）__。

（62）A．能及时抢占信道，但增加了冲突的概率

B．能及时抢占信道，并减少了冲突的概率

C．不能及时抢占信道，并增加了冲突的概率

D．不能及时抢占信道，但减少了冲突的概率

试题（62）分析

IEEE 802.3 定义的 CSMA/CD 协议中有三种监听算法，这三种监听算法的优缺点如下。

- 坚持型监听：能及时抢占信道，但增加了冲突的概率。
- 非坚持型监听：不能及时抢占信道，但减少了冲突的概率。
- P 坚持型监听：既能及时抢占信道，又能减少冲突的概率，但是算法复杂。

参考答案

（62）A

试题（63）

在千兆以太网物理层标准中，采用长波（1300nm）激光信号源的是＿（63）＿。

（63）A．1000Base-SX　　B．1000Base-LX
C．1000Base-CX　　D．1000Base-T

试题（63）分析

千兆以太网的物理层标准如下。

- 1000Base-CX：使用两对 STP 和 9 芯 D 型连接器，最大段长为 25m，适用于交换机之间短距离连接，例如千兆主干交换机和服务器之间的连接。
- 1000Base-LX：使用长波激光信号源，波长为 1270 nm～1355nm（1300nm），既可驱动多模光纤，也可驱动单模光纤。光纤规格如下。
  - 62.5μm 或 50μm 多模光纤，最大段长为 550m。
  - 9μm 的单模光纤，最长距离为 5km。
- 1000Base-SX：使用短波激光信号源，波长为 770 nm～860nm（为 800nm），可驱动多模光纤。光纤规格如下。
  - 62.5μm 的多模光纤，最大段长为 550m
  - 50μm 多模光纤，最大段长为 525m。
- 1000Base-TX：使用一对 5 类 UTP，最大段长为 100m。

参考答案

（63）B

试题（64）

以太网的最大帧长为 1518 字节，每个数据帧前面有 8 个字节的前导字段，帧间隔为 9.6μs，对于 10Base-5 网络来说，发送这样的帧需要多少时间？＿（64）＿

（64）A．1.23s　　B．12.3ms　　C．1.23ms　　D．1.23μs

试题（64）分析

10Base-5 以太网的数据速率是 10Mb/s，据此可以计算如下：

$$9.6\mu s+(8+1518)\times 8\div 10Mb/s=1230.4\mu s\approx 1.23ms$$

参考答案

（64）C

试题（65）

WLAN 采用扩频技术传输数据，下面哪一项不是扩频技术的优点？＿（65）＿

（65）A．对无线噪声不敏感　　B．占用的带宽小

C．产生的干扰小　　D．有利于安全保密

试题（65）分析

扩展频谱通信技术起初是为军事网络开发的，其主要想法是将信号散布到更宽的带宽上以减少发生阻塞和干扰的机会。早期的扩频方式是跳频扩频（FHSS），后来又有直接序列扩频（DSSS），这两种技术在 WLAN 中都有应用。扩展频谱系统的工作原理如图 6 所示。输入数据首先进入信道编码器，产生接近某中央频谱的较窄带宽的模拟信号，再用一个伪随机序列对这个信号进行调制。调制的结果是大大地拓宽了信号的带宽，即扩展了频谱。在接收端，使用同样的伪随机序列来恢复原来的信号，最后进入信道解码器来恢复数据。

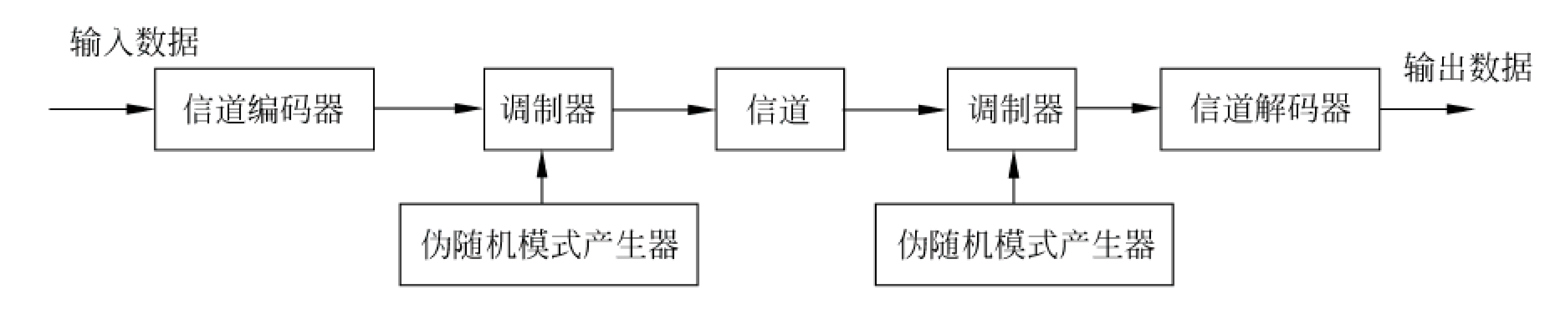


图 6　扩频系统工作原理

扩频技术的优点是对无线噪声不敏感，产生的干扰小，有利于安全保密。

参考答案

（65）B

试题（66）

建立一个家庭无线局域网，使得计算机不但能够连接因特网，而且 WLAN 内部还可以直接通信，正确的组网方案是＿（66）＿。

（66）A．AP+无线网卡　　B．无线天线+无线 MODEM

C．无线路由器+无线网卡　　D．AP+无线路由器

试题（66）分析

无线路由器是带有无线覆盖功能的路由器，它是将无线 AP 和宽带路由器合二为一的新型产品。它不仅具备无线 AP 的所有功能（如支持 DHCP 客户端、VPN 和 WEP 加密等），而且还包括了网络地址转换（NAT）功能，可实现家庭无线网络中的 Internet 连接共享，实现 ADSL 和小区宽带接入。

有的无线路由器还包括一个 4 端口的交换机，可以连接使用有线网卡的计算机，实现有线和无线网络的顺利过渡。在接入速度上，目前有符合 11Mb/s、54Mb/s 和 108Mb/s 的无线路由器产品。

参考答案

（66）C

试题（67）

计算机系统中广泛采用了 RAID 技术，在各种 RAID 技术中，磁盘容量利用率最低的是__（67）__。

（67）A．RAID0　　B．RAID1　　C．RAID3　　D．RAID5

试题（67）分析

RAID 为 Redundant Arrays of Independent Disks 的简称，中文为廉价冗余磁盘阵列。

RAID 0：将多个较小的磁盘合并成一个大的磁盘，不具有冗余，并行 I/O，速度最快，但可靠性最差。

RAID 1：两组相同的磁盘系统互作镜像，速度没有提高，但是允许单个磁盘出错，可靠性最好，但是其磁盘的利用率却只有 50%，是所有 RAID 上磁盘利用率最低的一个级别。

RAID 3：存放数据的原理和 RAID0、RAID1 不同。RAID 3 是以一个硬盘来存放数据的奇偶校验位，数据分段存储于其余硬盘中。利用单独的校验盘来保护数据虽然没有镜像的安全性高，但是硬盘利用率得到了很大的提高，为 n–1。

RAID 5：向阵列中的磁盘写数据，奇偶校验数据存放在阵列中的各个盘上，允许单个磁盘出错。RAID 5 也是以数据的校验位来保证数据的安全，但它不是以单独硬盘来存放数据的校验位，而是将数据段的校验位交互存放于各个硬盘上。这样，任何一个硬盘损坏，都可以根据其他硬盘上的校验位来重建损坏的数据。硬盘的利用率为 n–1。

参考答案

（67）B

试题（68）

以下协议中属于传输层的是__（68）__。

（68）A．UCP　　B．UDP　　C．TDP　　D．TDC

试题（68）分析

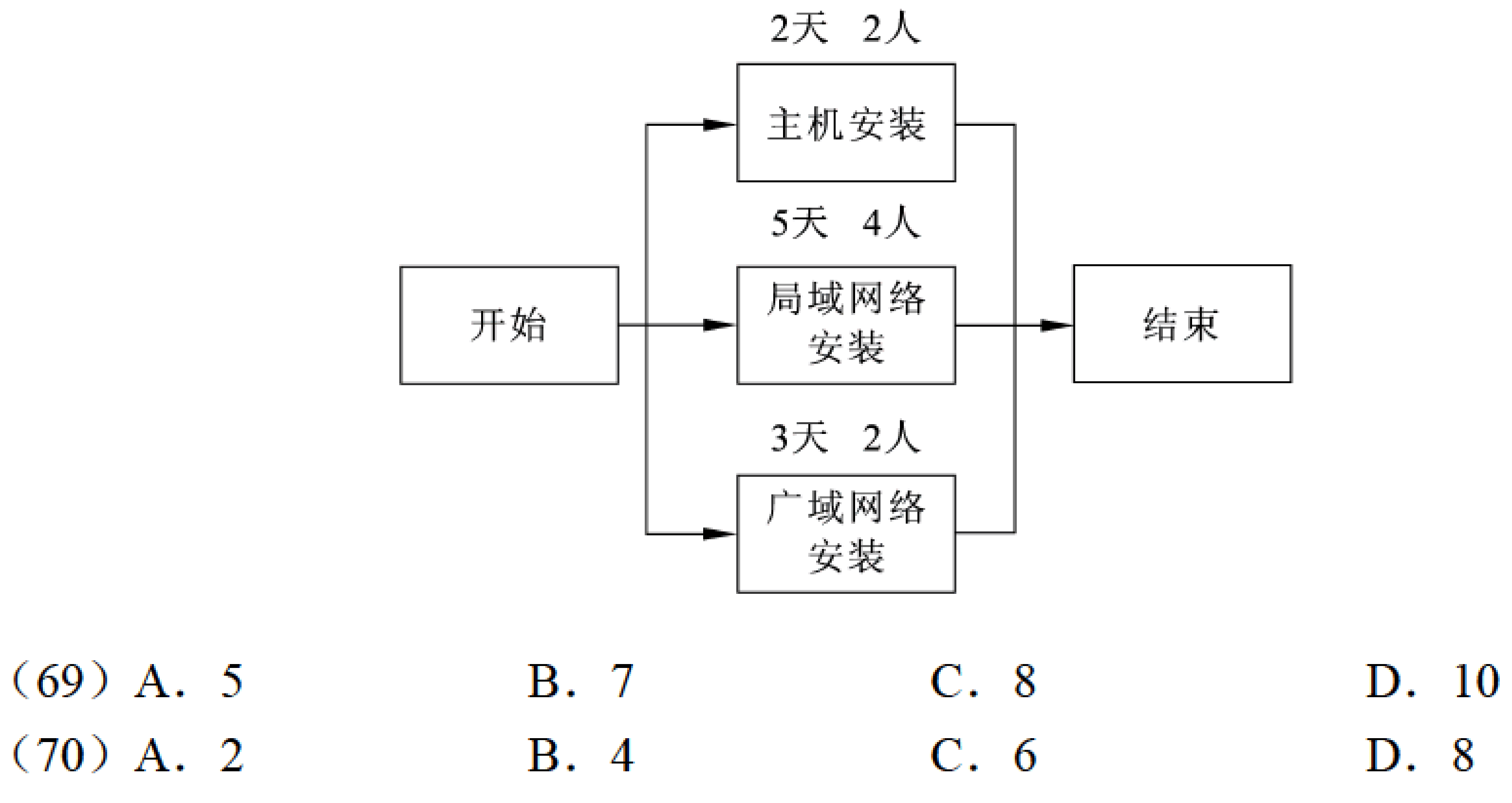
用户数据报协议（UDP）是 ISO 参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。UDP 协议基本上是 IP 协议与上层协议的接口。UDP 协议适用端口分辨运行在同一台设备上的多个应用程序。

参考答案

（68）B

试题（69）、（70）

下图为某系统集成项目的网络工程计划图，从图可知项目最短工期为__（69）__天，至少需要投入__（70）__人才能完成该项目（假设每个技术人员均能胜任每项工作）。



（69）A．5　　B．7　　C．8　　D．10

（70）A．2　　B．4　　C．6　　D．8

试题（69）、（70）分析

项目的进度管理需要兼顾时间和资源这两个因素，在分析项目进度计划的时候，要考虑资源使用的有效性，而人力资源是最主要的资源（并且一般会受到约束），一旦项目成员被分配到项目中，项目经理可以应用资源负荷和资源平衡两种方法最有效地调度团队成员。

资源负荷是指在特定的时间内现有的进度计划所需要的各种资源的数量，如在特定的时间内分配给某项工作的资源超过了项目的可用资源，就叫资源超负荷。为了消除超负荷，可以修改进度表，充分利用项目活动的浮动时间，通过延迟项目任务来解决资源冲突，这叫资源平衡，此时资源的利用达到了最佳的状态。

本题中网络图表示主机安装任务、局域网络安装任务和广域网络安装任务可以同时开始，而最长的路径是局域网络安装任务，整个项目的周期也就是总工期是 5 天。采用资源平衡方法，三个任务不同时进行，将广域网网络安装任务延迟两天（主机安装任务和局域网络安装任务同时开始），这样项目的进度是 5 天，但只需投入 6 个人就可以完成全部工作。

参考答案

（69）A　（70）C

试题（71）～（75）

Serialization delay and __(71)__ delay are the two components of network delay that are improved by increasing bandwidth. Serialization delay, i.e. the amount of time it takes to put the __(72)__ on the wire, and queuing delay (depth of the queue) are improved by increasing the __(73)__ from a 128Kbps circuit to a T1. However, three other components of delay, routing/switching delay, distance delay, and protocol delay are components that can not be positively affected by an __(74)__ in bandwidth. If the circuits are not over-utilized, then increasing the bandwidth to improve the __(75)__ of the application will only result in an

fincreased bandwidth with no positive effects on performance.

（71）A．buffering　　B．queuing　　C．receiving　　D．timing

（72）A．electricity　　B．digital　　C．data　　D．variable

（73）A. memory　　B．cache　　C．bandwidth　　D．delay

（74）A. increase　　B．decrease　　C．maintenance　　D．extension

（75）A．capability　　B．cost　　C．amount　　D．performance

参考译文

串行排序延迟和队列延迟是网络延迟的两个主要因素，这些是可以通过增加带宽加以改进的。串行排序延迟（将数据输出到线路上需要的时间）和队列延迟（队列的长度）可以通过把带宽从 128Kbps 增加到 T1 得到改善。然而，另外三种延迟因素——路由/交换延迟、距离延迟和协议处理延迟是不能通过增加带宽来改进的。如果线路没有超量使用，则通过增加带宽来改进应用软件性能的企图只能产生一种结果，那就是带宽的增加对性能并没有产生正面的影响。

参考答案

（71）B　（72）C　（73）C　（74）A　（75）D

第 12 章　2007 上半年网络工程师下午试题分析与解答

试题一（15 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某学校欲构建校园网，根据实际情况，计划在校园总部采用有线网络和无线网络相结合的接入方式，校园分部通过 Internet 采用 VPN 技术与校园总部互联，该校园网的网络拓扑结构如图 1-1 所示。

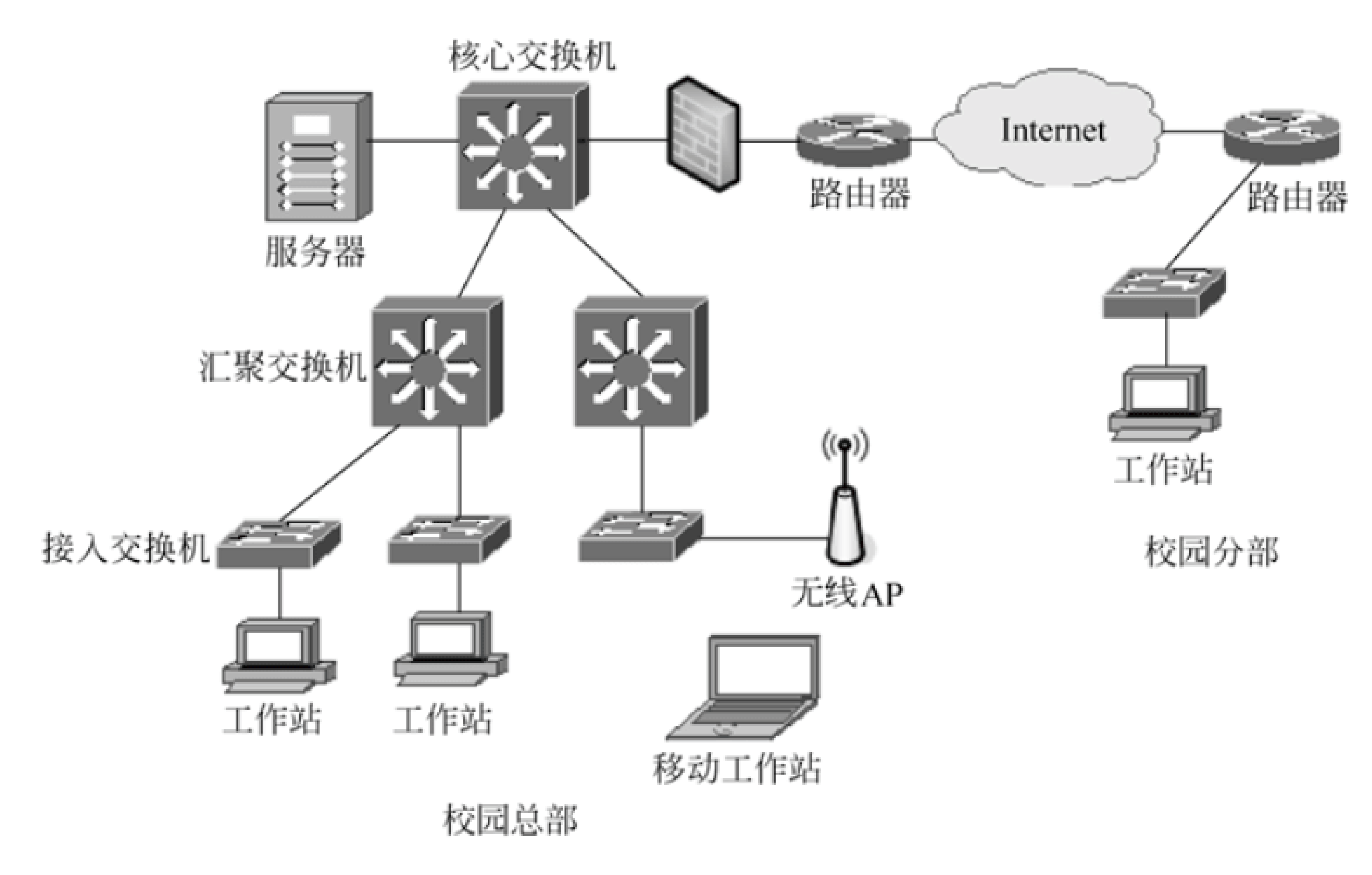


图 1-1

【问题 1】

从网络拓扑图中可以看出该校园网采用了分层设计结构，回答以下问题：

1．交换机按照所处的层次和完成的功能分为三种类型：核心交换机、汇聚交换机和接入交换机。下表是学校采购的三种交换机，请根据交换机的技术指标确定交换机的类型。在答题纸对应的解答栏内填写表 1-1 中（1）、（2）、（3）处对应的交换机类型（3 分）。

表 1-1

交换机类型	背板带宽	转发速率	接口介质	电源冗余	固定接口数量
（1）	1.2T	285MBPS	10/100/1000Base-T、1000FX	1+1	无
（2）	240G	100MBPS	1000FX	无	20 千兆光口
（3）	19G	6.6MBPS	100 Base-T、1000FX	无	24 百兆电口

2．该校园网根据需求使用 ACL 实现各个单位之间的访问控制，在能够实现预定功能的前提下，应将 ACL 交给__（4）__交换机实现，原因是__（5）__。（4 分）

（4）A．核心层　　B．汇聚层　　C．接入层

（5）A．核心层提供高速数据转发

B．汇聚层提供访问控制功能

C．接入层连接用户设备

【问题 2】

该校园网的部分区域采用了无线网络，请根据无线网络的技术原理回答以下问题：

1．校园网在部署无线网络时，采用了符合 802.11g 标准的无线网络设备，该校园网无线网络部分的最大数据速率为__（6）__。

（6）A．54Mb/s　　B．108Mb/s　　C．11Mb/s　　D．33Mb/s

2．在学校学术报告厅内部署了多个无线 AP，为了防止信号覆盖形成的干扰，应调整无线 AP 的__（7）__。

（7）A．SSID　　B．频道　　C．工作模式　　D．发射功率

【问题 3】

如果校园本部和校园分部之间需要实现教学资源互访、办公自动化和财务系统互联等多种业务，该校园网应该选择__（8）__VPN 模式。

（8）A．IPSec　　B．SSL

【问题 4】

该校园网本部利用 Windows 2000 建立 VPN 服务器，接受远程 VPN 访问，默认情况下，__（9）__接入到 VPN 服务器上。

（9）A．拒绝任何用户　　B．允许任何用户

C．除了 GUEST 用户，允许任何用户　　D．除了管理用户，拒绝任何用户

试题一分析

【问题 1】

本问题考查的是网络分层设计概念和网络设备基本参数的知识。

1．在网络分层设计中，由于核心层、汇聚层、接入层的功能不同，不同层次选用的交换机也有区别。

核心层的作用是尽可能快地交换数据包，构成高速的交换骨干，所以核心层交换机的背板带宽，转发速率尽可能快，另外，核心层可靠性要求较高，所以一般都要求电源冗余，现在核心层交换机一般不设置固定接口数量，这样可以根据用户的需要选配组件。

汇聚层主要提供地址的聚集，部门和工作组的接入，广播域、组播传输域的定义，VLAN 分割，介质转换和安全控制等功能。汇聚层是多台接入层交换机的汇聚点，它必须能够处理来自接入层设备的所有通信量，并提供到核心层的上行链路，因此汇聚层交

换机与接入层交换机比较，需要更高的性能，更少的接口和更高的交换速率。

接入层实现终端用户连接到网络，因此接入层交换机具有低成本和高端口密度特性。

从表 1-1 可见，根据上述三种交换机的特点，（1）对应核心层交换机；（2）对应汇聚层交换机；（3）对应接入层交换机。

2．由于核心层为下两层提供优化的数据转移功能，它是一个高速的交换骨干，其作用是尽可能快地交换数据包而不应卷入到具体数据包的运算中（如 ACL、过滤等），否则会降低数据包的交换速度。而分布层则提供基于统一策略的互连性，它连接核心层和接入层，对数据包进行复杂的运算，提供访问控制功能。

【问题 2】

本问题考查的是无线局域网的知识。

1．在 802.11 系列标准中，涉及物理层的有 802.11、802.11b、802.11a 和 802.11g 4 个标准。其中 802.11g 是对 802.11b 的一种高速物理层扩展，同 802.11b 一样，802.11g 工作于 2.4GHz ISM 频带，但采用了 OFDM 技术，可以实现最高 54Mb/s 的数据速率。

2．无线 AP 的发射功率决定了无线 AP 的覆盖范围。无线 AP 中 SSID（Service Set Identifier）也可以写为 ESSID，是用来区分不同的网络，它最多可以有 32 个字符。无线网卡设置不同的 SSID 就可以进入不同网络，无线 AP 的频道用于确定本网络工作的频率段，根据无线局域网的工作原理，在多个无线 AP 同时工作的情况下，为保证频道之间不相互干扰，要求两个频道的中心频率间隔不能低于 25MHz。为了防止信号覆盖形成的干扰，可以调节无线 AP 的频道。

【问题 3】

本问题考查的是 VPN 的知识。

目前实现 VPN 主要有 IPSecVPN 和 SSLVPN 两种模式。其中，SSLVPN 模式主要是实现 Web 应用，而其他应用还要使用 IPSecVPN 方式。从题目要求可以看出，该校园本部和校园分部之间需要实现教学资源互访、办公自动化和财务系统互联等多种应用，所以应该采用 IPSecVPN 方式。

【问题 4】

本问题考查的是 Windows 2000 建立 VPN 服务器的基本知识。

利用 Windows 2000 建立 VPN 服务器，接受远程 VPN 访问，默认情况下是拒绝任何用户访问的。

参考答案

【问题 1】

（1）核心交换机

（2）汇聚交换机

（3）接入交换机

（4）B 或汇聚层

（5）B 或汇聚层提供访问控制功能

【问题 2】

（6）A 或 54Mb/s

（7）B 或频道

【问题 3】

（8）A 或 IPSec

【问题 4】

（9）A 或拒绝任何用户

试题二（15 分）

阅读以下 Linux 系统中关于 IP 地址和主机名转换的说明，回答问题 1 至问题 3。

【说明】

计算机用户通常使用主机名来访问网络中的结点，而采用 TCP/IP 协议的网络是以 IP 地址来标记网络结点的，因此需要一种将主机名转换为 IP 地址的机制。在 Linux 系统中，可以使用多种技术来实现主机名和 IP 地址的转换。

【问题 1】

请选择恰当的内容填写在（1）、（2）、（3）空白处。

一般用 Host 表、网络信息服务系统（NIS）和域名服务（DNS）等多种技术来实现主机名和 IP 地址之间的转换。Host 表是简单的文本文件，而 DNS 是应用最广泛的主机名和 IP 地址的转换机制，它使用__（1）__来处理网络中成千上万个主机和 IP 地址的转换。在 Linux 中，DNS 是由 BIND 软件来实现的。BIND 是一个__（2）__系统， 其中的 resolver 程序负责产生域名信息的查询，一个称为__（3）__的守护进程，负责回答查询，这个过程称为域名解析。

（1）A．集中式数据库　B．分布式数据库

（2）A．C/S　B．B/S

（3）A．named　B．bind　C．nameserver

【问题 2】

下图是采用 DNS 将主机名解析成一个 IP 地址过程的流程图。请选择恰当的内容填写在（4）、（5）、（6）空白处。

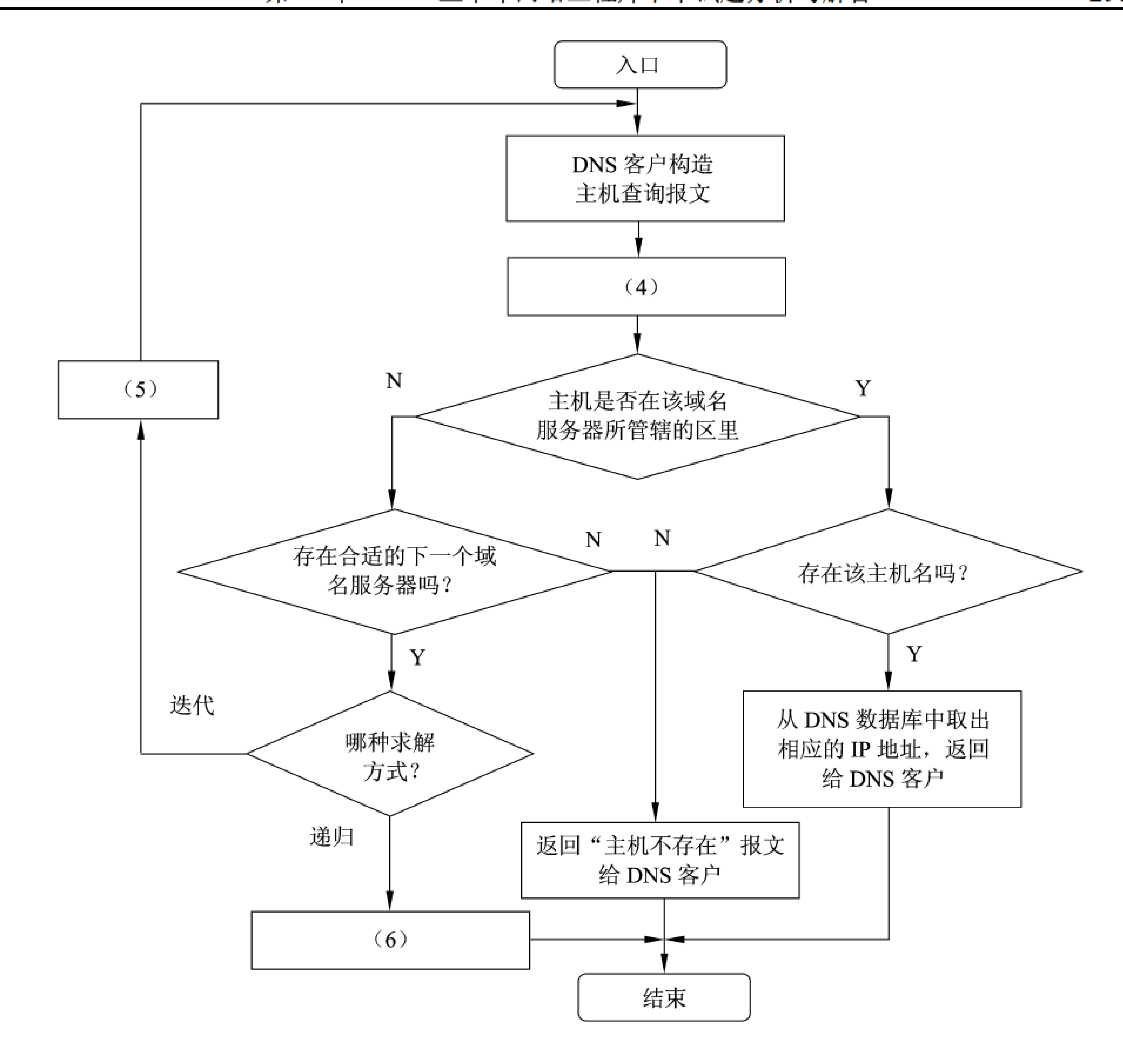
A．产生一个指定下一域名服务器的响应，送给 DNS 客户

B．把名字请求转送给下一个域名服务器，进行递归求解，结果返回给 DNS 客户

C．将查询报文发往某域名服务器

D．利用 Host 表查询

E．查询失败



【问题 3】

请在（7）、（8）、（9）处填写恰当的内容。

在 Linux 系统中设置域名解析服务器，已知该域名服务器上文件 named.conf 的部分内容如下：

```
options {
      directory '/var/named';
  };
  zone '.' {
      type hint;
      file 'named.ca';
  }
  zone 'localhost' IN {
      file "localhost.zone"
```

```
        allow-update{none;};
    };
    zone '0.0.127.in-addr.arpa'{
        type master;
        file 'named.local';
    };
    zone 'test.com'{
        type___(7)___;
        file 'test.com';
    };
    zone '40.35.222.in-addr.arpa'{
        type master;
        file '40.35.222';
    };
include "/etc/rndc.key";
```

该服务器是域 test.com 的主服务器，该域对应的网络地址是__(8)__，正向域名转换数据文件存放在__(9)__目录中。

试题二分析

【问题 1】

本问题考查对 TCP/IP 协议中 DNS（域名服务）基本概念的理解。

为了便于记忆，计算机用户通常使用主机名来访问网络中的计算机，需要一种将主机名转换为 IP 地址的机制。目前主要有三种技术来实现主机名和 IP 地址之间的转化，Host 表、NIS（网络信息服务系统）和 DNS 域名服务。

Host 表是简单的文本文件，在 Linux 系统中是/etc/hosts 文件，其中存放了主机名和 IP 地址的映射关系。而在一个大型的网络中建立 host 表非常繁杂。NIS（Network Information System）将主机表以数据库的形式保存在中央主机上，由中央主机将所需数据分配给所有的服务器，主机名转换为 IP 的效率很低，适用于局域网。TCP/IP 网络系统中实用的 IP 地址和主机名的转换机制是 DNS（Domain Name Server），它使用一种分层的分布式数据库来处理地址和名字的转换，转换信息分布在一个层次结构的若干台域名服务器上。

DNS 基于客户/服务器模式。每当一个应用需要将域名翻译为 IP 地址时，由 DNS 客户程序将待翻译的域名放在一个 DNS 请求信息中，域名服务器系统从这个请求中取出域名，通过递归或迭代查询方式，返回给客户翻译好的 IP 地址（或查询失败）结果。

在 Linux 中，域名服务（DNS）是由 BIND（Berkeley Internet Name Domain）软件实现的。BIND 是一个 C/S 系统，其客户端称为转换程序（resolver），它负责产生域名信息的查询，并将这类信息发送给服务器。BIND 的服务器端是一个称为 named 的守护进程，负责回答转换程序的查询。

【问题 2】

DNS 客户需要向 DNS 系统查询主机 IP 地址时，首先构造名字查询报文，然后根据客户机的网络配置中指定的 DNS 服务器地址，将查询报文发送给 DNS 服务器，DNS 服务器有两种处理方式，一种是递归查询，当收到 DNS 工作站的查询请求后，如本地 DNS 服务器查询成功则返回客户端查询结果，如本地查询失败，由本地域名服务器利用服务器上的软件采用递归算法请求下一个服务器（将查询请求向下一个 DNS 服务器转发），并将结果返回查询客户。另一种是迭代查询，当收到 DNS 工作站的查询请求后，如果 DNS 服务器中没有查到所需 IP 地址，该 DNS 服务器将告知另外一台 DNS 服务器的 IP 地址，然后再由 DNS 工作站自行向此 DNS 服务器查询，直到查到所需信息为止（或者失败）。一般在 DNS 服务器之间的查询请求便属于迭代查询。

【问题 3】

BIND 域名服务器的守护进程是 named，其主要配置文件是/etc/named.conf，在启动时 named 服务程序读取该配置文件来决定应该如何工作。

named.conf 文件由语句（起作用的命名配置）、注释和空行组成。常用语句的声明如下。

options 语句，允许为名字服务器设置全局选项，通常在 options{　}语句块中指定名字服务器的工作目录路径（设置 directory 目录选项）、转发 DNS 查询的 IP 地址表（设置 forwarders 选项）等。

在多个 zone 语句中定义区域文件，指出某个域的地址转换配置信息（或者反向转换配置信息）存放的数据库文件名称和类型，如果为特定的域设置多个名字服务器，可以使用 type master 选项只设置其中一个为主要的或授权名字服务器，其他名字服务器（个数不限）必须设置为从名字服务器（type slave）。反向 DNS 区域（通过 IP 地址查询主机名称为反向查询，查询信息在反向 DNS 区域文件中）配置采用特殊的区域名字，要求把网络 IP 地址的分段数字“反向”并在名字的最后增加 in-addr.arpa 来创建反向 DNS 区域名字，该文件的数字串（用点符号分割）从右到左就是由该区域文件管理网络域的网络地址。

参考答案

【问题 1】

（1）B，或分布式数据库

（2）A 或 C/S，或客户/服务器系统

（3）A 或 named

【问题 2】

（4）C 将查询报文发往某域名服务器

（5）A 产生一个指定下一域名服务器的响应，送给 DNS 客户

（6）B 把名字请求转送给下一个域名服务器，进行递归求解，结果返回给 DNS 客户

【问题 3】

（7）master

（8）222.35.40.0

（9）/var/named

试题三（15 分）

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】

某网络拓扑结构如图 3-1 所示，DHCP 服务器分配的地址范围如图 3-2 所示。

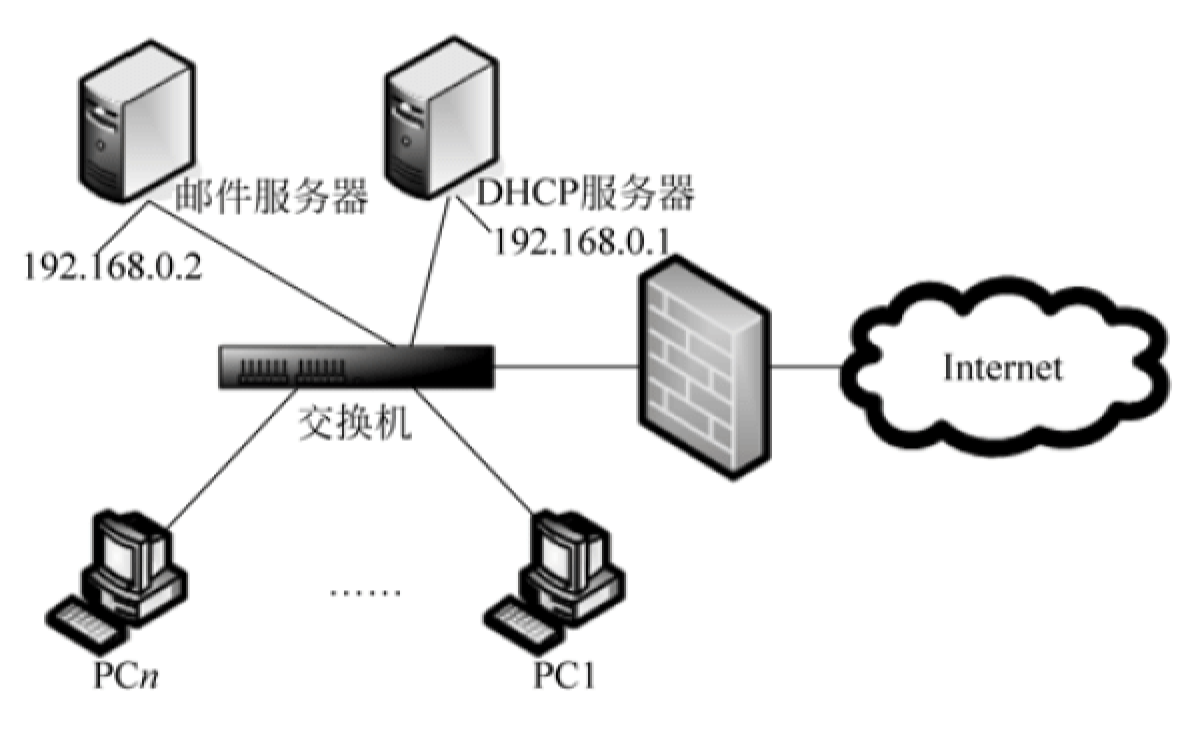


图 3-1

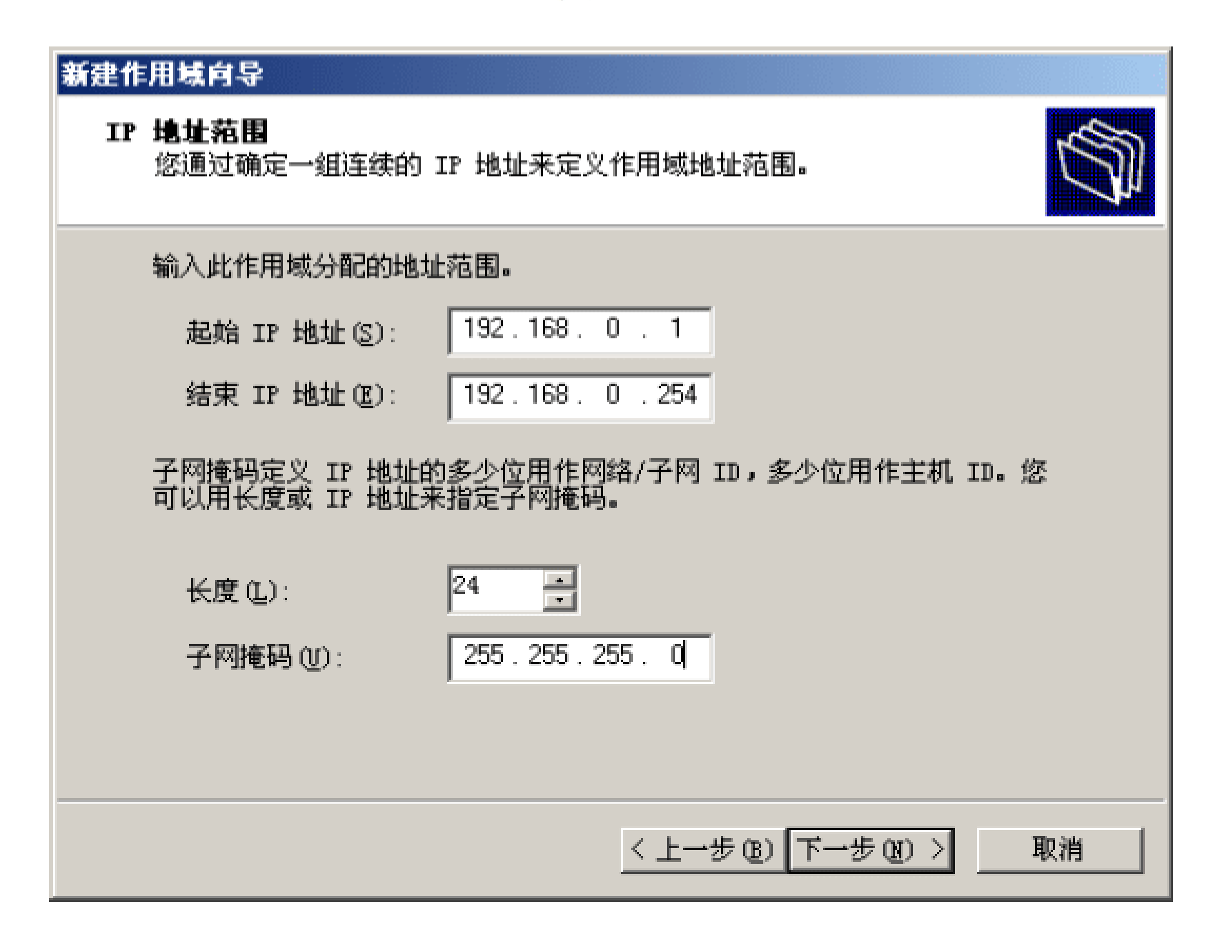


图 3-2

【问题 1】

DHCP 允许服务器向客户端动态分配 IP 地址和配置信息。客户端可以从 DHCP 服务器获得__（1）__。

（1）A．DHCP 服务器的地址　B．Web 服务器的地址　C．DNS 服务器的地址

【问题 2】

图 3-3 是 DHCP 服务器安装中的添加排除窗口。

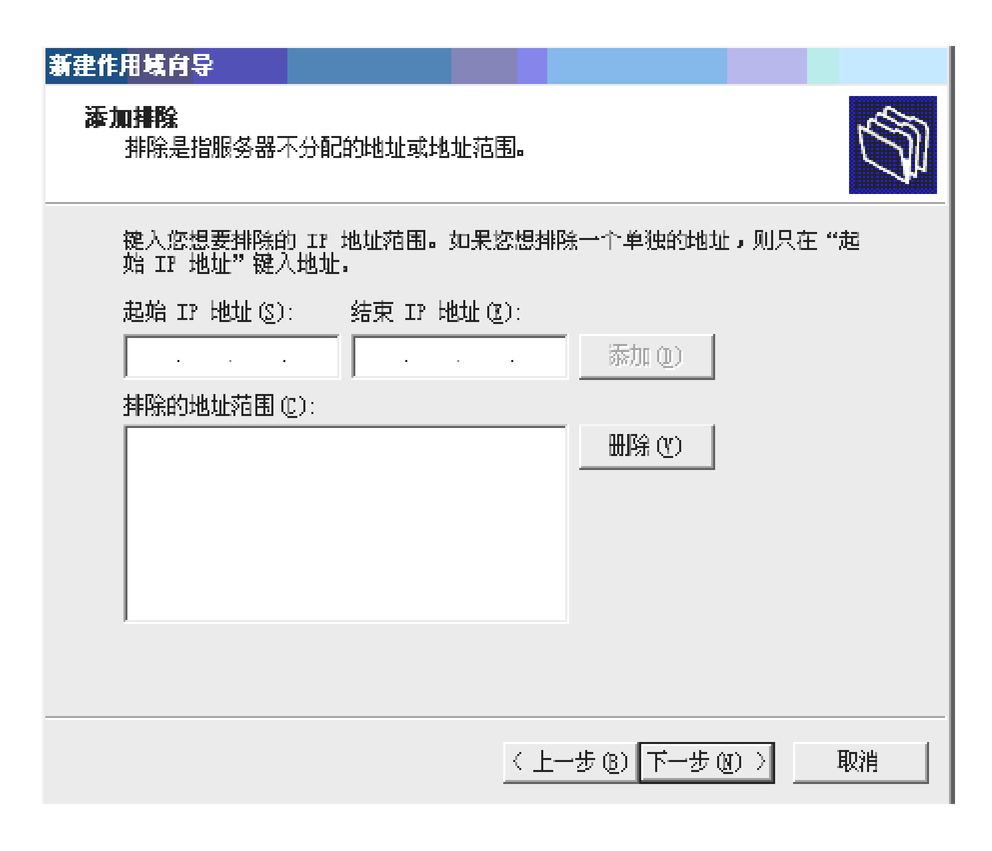


图 3-3

参照图 3-1 和图 3-2，为图 3-3 中配置相关信息。

起始 IP 地址：　__（2）__；

结束 IP 地址：　__（3）__；

【问题 3】

在 DHCP 服务器安装完成后，DHCP 控制台如图 3-4 所示。

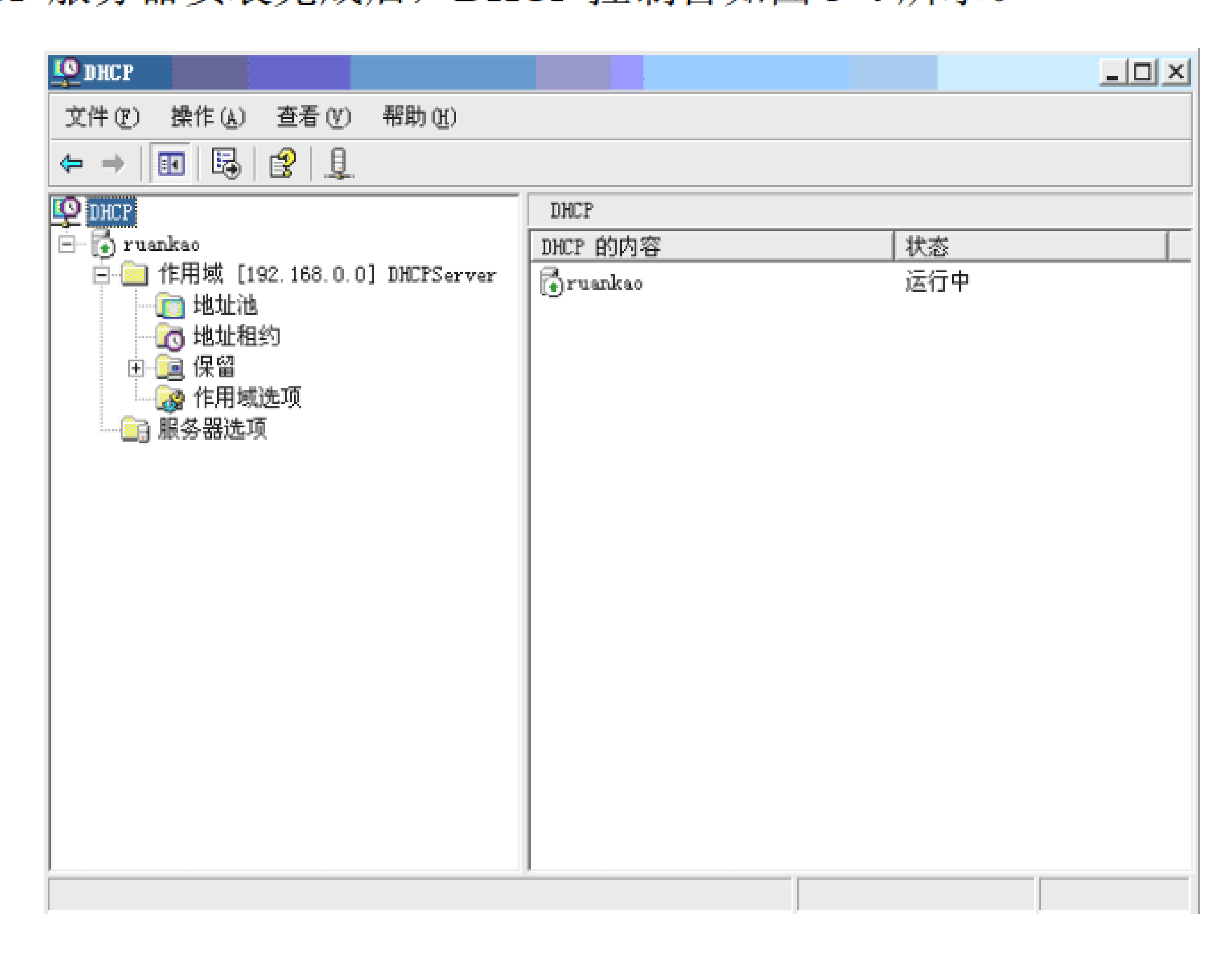


图 3-4

配置 DHCP 服务器时需要进行备份，以备网络出现故障时能够及时恢复。在图 3-4 中，备份 DHCP 服务器配置信息正确的方法是__（4）__。

（4）A．右键单击“ruankao”服务器名，选择“备份”

B．右键单击“作用域”，选择“备份”

C．右键单击“作用域选项”，选择“备份”

D．右键单击“服务器选项”，选择“备份”

【问题 4】

通常采用 IP 地址与 MAC 地址绑定的策略为某些设备保留固定的 IP 地址。右键单击图 3-4 中的__（5）__选项可进行 IP 地址与 MAC 地址的绑定设置。

（5）A．地址池　　B．地址租约　　C．保留　　D．作用域选项

【问题 5】

邮件服务器的网络配置信息如图 3-5 所示。请在图 3-6 中为邮件服务器绑定 IP 地址和 MAC 地址。

IP 地址：__（6）__；

MAC 地址：__（7）__。



图 3-5

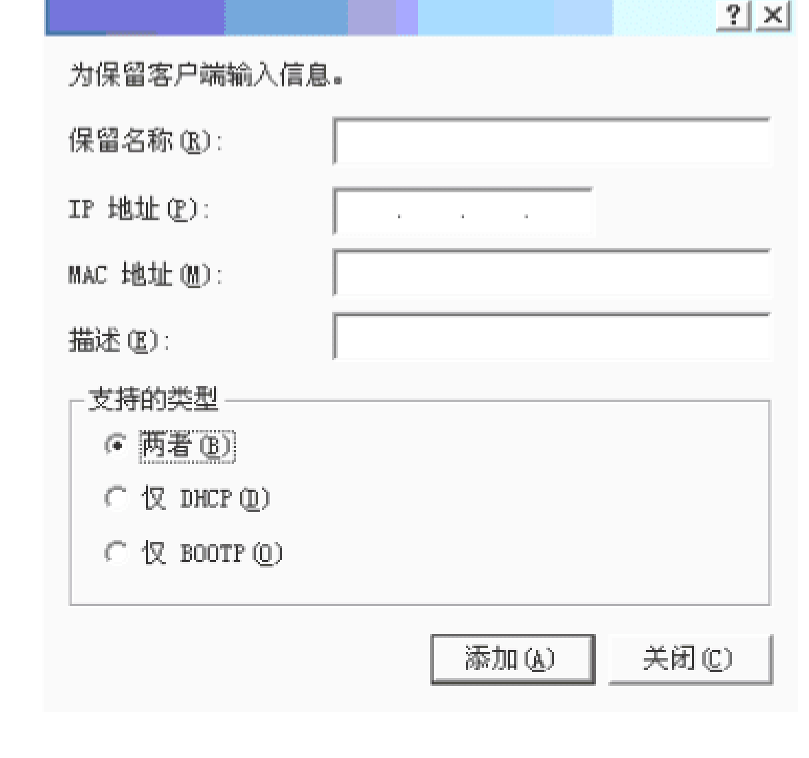


图 3-6

试题三分析

【问题 1】

DHCP 是 Dynamic Host Configuration Protocol（动态主机配置协议）的缩写。在常见的小型网络中，IP 地址的分配一般都采用静态方式，但在大中型网络中，为每一台计算机分配一个静态 IP 地址，这样将会加重网管人员的负担，并且容易导致 IP 地址分配错误。因此，在大中型网络中使用 DHCP 服务是非常有效率的。

DHCP 客户端通过和 DHCP 服务器的交互通信以获得 IP 地址租约，包括 IP 地址、

子网掩码以及 DNS 服务器的地址。

【问题 2】

由于 IP 地址 DHCP 服务器（192.168.0.1）和邮件服务器（192.168.0.2）的 IP 地址需静态分配，故在添加排除窗口中应将它们排除掉，因此起始 IP 地址应填入 192.168.0.1，结束 IP 地址应填入 192.168.0.2。

【问题 3】

在网络管理工作中，备份一些必要的配置信息是一项重要的工作，以便当网络出现故障时，能够及时地恢复正确的配置信息，保障网络正常的运转。在配置 DHCP 服务器时也不例外，Windows 2003 服务器操作系统中，也为用户提供了备份和还原 DHCP 服务器配置的功能。

（1）打开 DHCP 控制台，在控制台窗口中，展开“DHCP”选项，选择已经建立好的 DHCP 服务器，右键单击服务器名，选择“备份”。

（2）这时便会弹出一个要求用户选择备份路径的对话框。默认情况下，DHCP 服务器的配置信息是放在系统安装盘的“windows\system32\dhcp\backup”目录下。如有必要，用户可以手动更改备份的位置。单击“确定”按钮后就完成了对 DHCP 服务器配置文件的备份工作，如下图所示。



选择要备份配置文件的位置

（3）当出现配置故障时，需要还原 DHCP 服务器的配置信息，右键单击 DHCP 服务器名，选择“还原”选项即可，同样会有一个确定还原位置的选项，选择备份时使用的文件夹单击“确定”按钮，这时会打开一个“关闭和重新启动服务”的对话框，单击“确定”按钮后，DHCP 服务器就会自动恢复到最初的备份配置。

故右键单击“ruankao”服务器名，选择“备份”。

【问题 4】

右键单击“保留”选项，可填写需保留 IP 地址的信息。

【问题 5】

在 DHCP 服务器中，通常会保留一些 IP 地址给一些特殊用途的网络设备，如路由器、打印服务器等，如果客户机私自将自己的 IP 地址更改为这些地址，就会造成这些设备无法正常工作。这时，就需要合理配置这些 IP 地址与 MAC 地址进行绑定，来防止保留的 IP 地址被盗用。步骤如下。

（1）了解客户机的 MAC 地址。在想要实现绑定的客户机的“开始”、“运行”中输入 CMD 命令，打开 Windows 2003 的命令提示符窗口。然后输入“IPCONFIG /ALL”查看网络的配置信息，其中有一项 NIC 后面的十六进制数便是这台机器的 MAC 地址信息，如图 3-5 所示。

（2）实现 IP 地址与 MAC 地址绑定策略。打开 DHCP 服务器控制台，展开已经建立好的 DHCP 服务器，右键单击“保留”选项，这时选择“新建保留”选项。在“保留名称”文本框中输入保留的计算机名，在“IP 地址”文本框中，输入需要绑 MAC 地址的 IP 地址；在“MAC 地址”文本框中，输入需要绑定主机的 MAC 地址。这样，就为网络设备添加了一个 MAC 地址绑定，如图 3-6 所示。

参考答案

【问题 1】

（1）C

【问题 2】

（2）192.168.0.1

（3）192.168.0.2

【问题 3】

（4）A

【问题 4】

（5）C

【问题 5】

（6）192.168.0.2

（7）00-16-36-33-9B-BE

试题四（15 分）

阅读下列有关网络防火墙的说明，回答问题 1 至问题 4，将答案填入答题纸对应的解答栏内。

【说明】

为了保障内部网络的安全，某公司在 Internet 的连接处安装了 PIX 防火墙，其网络结构如图 4-1 所示。

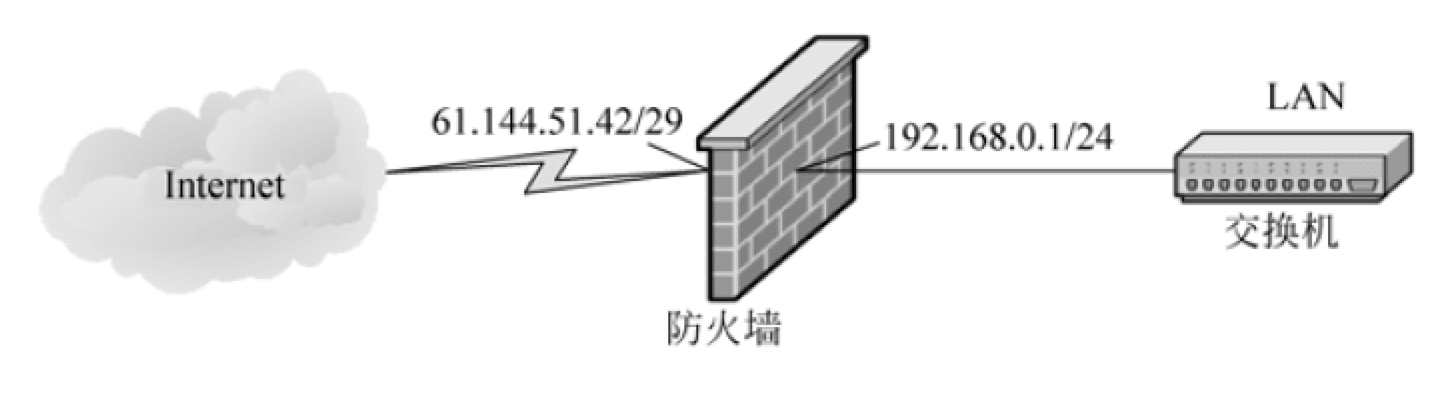


图 4-1

【问题 1】

完成下列命令行，对网络接口进行地址初始化配置。

firewall(config)#ip address inside ＿（1）＿ ＿（2）＿

firewall(config)#ip address outside ＿（3）＿ ＿（4）＿

【问题 2】

阅读以下防火墙配置命令，为每条命令选择正确的解释。

firewall(config)#global (outside) 1　61.144.51.46 ＿（5）＿

firewall(config)#nat (inside) 1　0.0.0.0　0.0.0.0 ＿（6）＿

firewall(config)#static (inside, outside) 192.168.0.8 61.144.51.43 ＿（7）＿

（5）A．当内网的主机访问外网时，将地址统一映射为 61.144.51.46

B．当外网的主机访问内网时，将地址统一映射为 61.144.51.46

C．设定防火墙的全局地址为 61.144.51.46

D．设定交换机的全局地址为 61.144.51.46

（6）A．启用 NAT，设定内网的 0.0.0.0 主机可访问外网 0.0.0.0 主机

B．启用 NAT，设定内网的所有主机均可访问外网

C．对访问外网的内网主机不作地址转换

D．对访问外网的内网主机进行任意的地址转换

（7）A．地址为 61.144.51.43 的外网主机访问内网时，地址静态转换为 192.168.0.8

B．地址为 61.144.51.43 的内网主机访问外网时，地址静态转换为 192.168.0.8

C．地址为 192.168.0.8 的外网主机访问外网时，地址静态转换为 61.144.51.43

D．地址为 192.168.0.8 的内网主机访问外网时，地址静态转换为 61.144.51.43

【问题 3】

管道命令的作用是允许数据流从较低安全级别的接口流向较高安全级别的接口。解释或完成以下配置命令。

firewall(config)#conduit permit tcp host 61.144.51.43 eq www any ＿（8）＿

firewall(config)#＿（9）＿　允许 icmp 消息任意方向通过防火墙

【问题 4】

以下命令针对网络服务的端口配置，解释以下配置命令：

firewall(config)#fixup protocol http 8080 ____（10）____

firewall(config)#no fixup protocol ftp 21 ____（11）____

试题四分析

【问题 1】

本问题考查的是 PIX 防火墙中配置内外网卡的 IP 地址（ip address）命令。

例如：

```
firewall(config)#ip address outside 61.144.51.42 255.255.255.248
firewall (config)#ip address inside 192.168.0.1 255.255.255.0
```

表明防火墙在外网的 IP 地址是 61.144.51.42，内网 IP 地址是 192.168.0.1。

【问题 2】

本问题考查的是 PIX 防火墙中配置地址转换、外部地址范围和静态地址翻译的命令。

1．指定要进行转换的内部地址（nat）

网络地址翻译（nat）作用是将内网的私有 IP 转换为外网的公有 ip.Nat 命令总是与 global 命令一起使用，这是因为 nat 命令可以指定一台主机或一段范围的主机访问外网，访问外网时需要利用 global 所指定的地址池进行对外访问。nat 命令配置语法：nat (if_name) nat_id local_ip [netmark]。

其中（if_name）表示内网接口名字，例如 inside. Nat_id 用来标识全局地址池，使它与其相应的 global 命令相匹配，local_ip 表示内网被分配的 IP 地址。例如 0.0.0.0 表示内网所有主机可以对外访问。[netmark]表示内网 IP 地址的子网掩码。

例 1．Pix525(config)#nat (inside) 1 0 0

表示启用 nat，内网的所有主机都可以访问外网，用 0 可以代表 0.0.0.0。

例 2．Pix525(config)#nat (inside) 1 172.16.5.0 255.255.0.0

表示只有 172.16.5.0 这个网段内的主机可以访问外网。

2．指定外部地址范围（global）

global 命令把内网的 IP 地址翻译成外网的 IP 地址或一段地址范围。Global 命令的配置语法：global (if_name) nat_id ip_address-ip_address [netmark global_mask]。

其中（if_name）表示外网接口名字，例如 outside.。Nat_id 用来标识全局地址池，使它与其相应的 nat 命令相匹配，ip_address-ip_address 表示翻译后的单个 IP 地址或一段 IP 地址范围。[netmark global_mask]表示全局 IP 地址的网络掩码。

例 1．Pix525(config)#global (outside) 1 61.144.51.42-61.144.51.48

表示内网的主机通过 pix 防火墙要访问外网时，pix 防火墙将使用 61.144.51.42-61.144.51.48 这段 IP 地址池为要访问外网的主机分配一个全局 IP 地址。

例 2．Pix525(config)#global (outside) 1 61.144.51.42

表示内网要访问外网时，pix 防火墙将为访问外网的所有主机统一使用 61.144.51.42

这个单一 IP 地址。

例 3．Pix525(config)#no global (outside) 1 61.144.51.42

表示删除这个全局表项。

3．配置静态 IP 地址翻译（static）

如果从外网发起一个会话，会话的目的地址是一个内网的 IP 地址，static 就把内部地址翻译成一个指定的全局地址，允许这个会话建立。static 命令配置语法：static (internal_if_name，external_if_name) outside_ip_address inside_ ip_address。其中 internal_if_name 表示内部网络接口，安全级别较高。inside. external_if_name 为外部网络接口，安全级别较低，如 outside 等。outside_ip_address 为正在访问的较低安全级别的接口上的 IP 地址。inside_ ip_address 为内部网络的本地 IP 地址。

例 1．Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.8

表示 IP 地址为 192.168.0.8 的主机，对于通过 pix 防火墙建立的每个会话，都被翻译成 61.144.51.62 这个全局地址，也可以理解成 static 命令创建了内部 IP 地址 192.168.0.8 和外部 IP 地址 61.144.51.62 之间的静态映射。

例 2．Pix525(config)#static (inside, outside) 192.168.0.2 10.0.1.3

例 3．Pix525(config)#static (dmz, outside) 211.48.16.2 172.16.10.8

注释同例 1。通过以上几个例子说明使用 static 命令可以让用户为一个特定的内部 IP 地址设置一个永久的全局 IP 地址。这样就能够为具有较低安全级别的指定接口创建一个入口，使它们可以进入到具有较高安全级别的指定接口。

【问题 3】

本问题考查的是 PIX 防火墙中的管道命令（conduit）。

前面讲过使用 static 命令可以在一个本地 IP 地址和一个全局 IP 地址之间创建一个静态映射，但从外部到内部接口的连接仍然会被 pix 防火墙的自适应安全算法（ASA）阻挡。conduit 命令用来允许数据流从具有较低安全级别的接口流向具有较高安全级别的接口，例如允许从外部到 DMZ 或内部接口的进入方向的会话。对于向内部接口的连接，static 和 conduit 命令将一起使用，来指定会话的建立。

conduit 命令配置语法：

```
conduit permit | deny global_ip port[-port] protocol foreign_ip [netmask]
```

permit | deny 允许 | 拒绝访问

global_ip 指的是先前由 global 或 static 命令定义的全局 IP 地址，如果 global_ip 为 0，就用 any 代替 0；如果 global_ip 是一台主机，就用 host 命令参数。

port 指的是服务所作用的端口，例如 www 使用 80，smtp 使用 25 等，用户可以通过服务名称或端口数字来指定端口。

protocol 指的是连接协议，如 TCP、UDP 和 ICMP 等。

foreign_ip 表示可访问 global_ip 的外部 IP。对于任意主机，可以用 any 表示。如果

foreign_ip 是一台主机，就用 host 命令参数。

例 1．Pix525(config)#conduit permit tcp host 192.168.0.8 eq www any

这个例子表示允许任何外部主机对全局地址 192.168.0.8 的这台主机进行 http 访问。其中使用 eq 和一个端口来允许或拒绝对这个端口的访问。Eq ftp 就是指允许或拒绝只对 ftp 的访问。

例 2．Pix525(config)#conduit deny tcp any eq ftp host 61.144.51.89

表示不允许外部主机 61.144.51.89 对任何全局地址进行 ftp 访问。

例 3．Pix525(config)#conduit permit icmp any any

表示允许 icmp 消息向内部和外部通过。

例 4．Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.3

Pix525(config)#conduit permit tcp host 61.144.51.62 eq www any

这个例子说明 static 和 conduit 的关系。192.168.0.3 在内网是一台 Web 服务器，现在希望外网的用户能够通过 pix 防火墙得到 Web 服务。所以先做 static 静态映射：192.168.0.3—>61.144.51.62（全局），然后利用 conduit 命令允许任何外部主机对全局地址 61.144.51.62 进行 http 访问。

【问题 4】

本问题考查的是 PIX 防火墙中的配置 fixup 协议命令。

fixup 命令的作用是启用，禁止，改变一个服务或协议通过 pix 防火墙，由 fixup 命令指定的端口是 pix 防火墙要侦听的服务。见下面例子。

例 1．Pix525(config)#fixup protocol ftp 21

启用 ftp 协议，并指定 ftp 的端口号为 21。

例 2．Pix525(config)#fixup protocol http 80

Pix525(config)#fixup protocol http 1080

为 HTTP 协议指定 80 和 1080 两个端口。

例 3．Pix525(config)#no fixup protocol smtp 80

禁用 smtp 协议。

参考答案

【问题 1】

（1）修改主机名为 SwitchA

（2）进入 VLAN 配置子模式

（3）设置本交换机为 Server 模式

（4）设置域名为 vtpserver

（5）启动修剪功能

【问题 2】

（6）mode trunk

（7）vlan all

【问题 3】

（8）switchport mode access

（9）switchport access vlan 10

【问题 4】

（10）128

（11）e0/3（答 f0/3 或端口 3 也正确）

试题五（15 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

图 5-1 是 VLAN 配置的结构示意图。

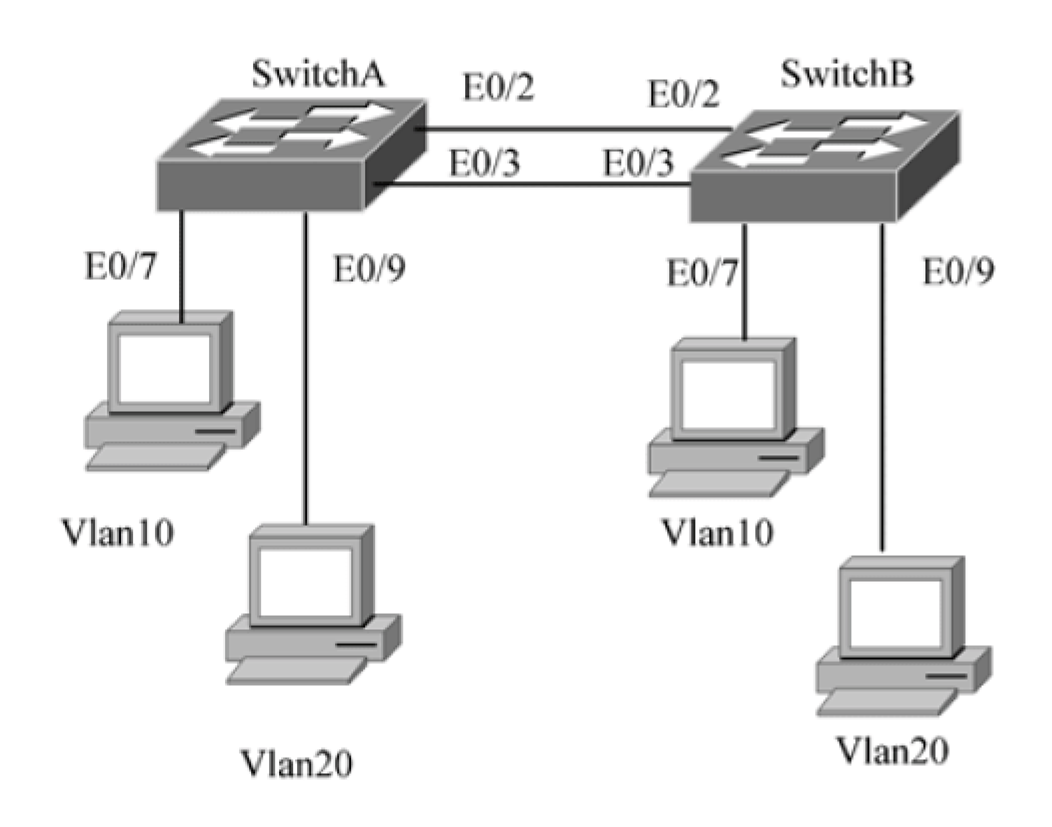


图 5-1

【问题 1】

请阅读下列 Switch A 的配置信息，并在（1）～（5）处解释该语句的作用。

```
Switch>enable                               (进入特权模式)
Switch#config terminal                      (进入配置模式)
Switch(config)#hostname SwitchA             ___(1)___
SwitchA (config)#end
SwitchA #
SwitchA #vlan database                      ___(2)___
SwitchA (vlan)#vtp server                   ___(3)___
SwitchA (vlan)#vtp domain vtpserver         ___(4)___
SwitchA (vlan)#vtp pruning                  ___(5)___
SwitchA (vlan)#exit                         (退出 VLAN 配置模式)
```

【问题 2】

下面是交换机完成 Trunk 的部分配置，请根据题目要求，完成下列配置。

```
SwitchA (config)#interface f0/3                (进入端口 3 配置模式)
SwitchA (config-if)#switchport___(6)___        (设置当前端口为 Trunk 模式)
SwitchA (config-if)# switchport trunk allowed___(7)___   (设置允许所有 Vlan 通过)
SwitchA (config-if)#exit
SwitchA (config)#exit
Switch#
```

【问题 3】

下面是交换机完成端口配置的过程，请根据题目要求，完成下列配置。

```
Switch(config)#interface f0/7                  (进入端口 7 的配置模式)
Switch(config-if)# ___(8)___                   (设置端口为静态 VLAN 访问模式)
Switch(config-if)# ___(9)___                   (把端口 7 分配给 VLAN10)
Switch(config-if)#exit
Switch(config)#exit
```

【问题 4】

下面是基于端口权值的负载均衡配置过程。

```
SwitchA(config)#interface f0/2                 (进入端口 2 配置模式)
SwitchA(config-if)# spanning-tree vlan 10 port-priority 10  (将 VLAN10 的端口权值设为 10)
SwitchA(config-if)#exit
SwitchA(config)#interface f0/3                 (进入端口 3 配置模式)
SwitchA(config-if)# spanning-tree vlan 20 port-priority 10  (将 VLAN20 的端口权值设为 10)
Switch1(config-if)#end
Switch1#copy running-config startup-config     (保存配置文件)
```

1．不同 Trunk 上不同 VLAN 的权值不同，在默认情况下，其权值为___(10)___。

2．按照上述配置，Vlan20 的数据通过 Switch A 的___(11)___口发送和接收数据。

试题五分析

【问题 1】

本问题考查的是交换机的基本配置知识。各命令功能如下。

```
Switch>enable                        进入特权模式
Switch#config terminal               进入配置模式
Switch(config)#hostname SwitchA      修改主机名为 SwitchA
```

```
SwitchA (config)#end
SwitchA #
SwitchA #vlan database                        进入 VLAN 配置子模式
SwitchA (vlan)#vtp server                     设置本交换机为 Server 模式
SwitchA (vlan)#vtp domain vtpserver           设置域名为 vtpserver
SwitchA (vlan)#vtp pruning                    启动修剪功能
SwitchA (vlan)#exit                           退出 VLAN 配置模式
```

【问题 2】

本问题考查的是交换机的 Trunk 的配置。配置命令及解释如下。

```
SwitchA (config)#interface f0/3               （进入端口 3 配置模式）
SwitchA (config-if)#switchport mode trunk     （设置当前端口为 Trunk 模式）
SwitchA (config-if)# switchport trunk allowed vlan all  （设置允许所有
                                                          Vlan 通过）
SwitchA (config-if)#exit
SwitchA (config)#exit
Switch#
```

【问题 3】

本问题考查的是将端口划入 VPN 的基本操作。其命令及解释如下。

```
Switch(config)#interface f0/7                 （进入端口 7 的配置模式）
Switch(config-if)# switchport mode access     （设置端口为静态 VLAN 访问模式）
Switch(config-if)# switchport access vlan 10     （把端口 7 分配给 VLAN10）
Switch(config-if)#exit
Switch(config)#exit
```

【问题 4】

本问题考查的是端口权值的负载均衡配置。

默认情况下端口权值为 128，STP 协议可以根据权值的大小来使不同 Trunk 发送和接收不同 VLAN 的数据，来实现负载均衡的目的。

```
SwitchA(config)#interface f0/2                         （进入端口 2 配置模式）
SwitchA(config-if)# spanning-tree vlan 10 port-priority 10 （将 VLAN10
的端口权值设为 10）
SwitchA(config-if)#exit
SwitchA(config)#interface f0/3                         （进入端口 3 配置模式）
SwitchA(config-if)# spanning-tree vlan 20 port-priority 10 （将 VLAN20
的端口权值设为 10）
Switch1(config-if)#end
```

按照上面的配置，Vlan20 在端口 3 的权值为 10，在其他端口的权值为默认值，故 Vlan20 的数据通过 Switch A 的端口 3 收发数据。

参考答案

【问题 1】

（1）修改主机名为 SwitchA

（2）进入 VLAN 配置子模式

（3）设置本交换机为 Server 模式

（4）设置域名为 vtpserver

（5）启动修剪功能

【问题 2】

（6）mode trunk

（7）vlan all

【问题 3】

（8）switchport mode access

（9）switchport access vlan 10

【问题 4】

（10）128

（11）e0/3（答 f0/3 或 端口 3 也正确）

第 13 章　2007 下半年网络工程师上午试题分析与解答

试题（1）

若某计算机系统由两个部件串联构成，其中一个部件的失效率为 7×10^{-6}/小时。若不考虑其他因素的影响，并要求计算机系统的平均故障间隔时间为 10^{5} 小时，则另一个部件的失效率应为__（1）__/小时。

（1）A．2×10^{-5}　　B．3×10^{-5}　　C．4×10^{-6}　　D．3×10^{-6}

试题（1）分析

根据题意，该计算机系统的总失效率为系统平均故障间隔时间的倒数，即 10^{-5}/小时。而计算机系统的总失效率又是各部件失效率的和。因此，另一个部件的效率最大为 10^{-5}/H-7×10^{-6}/H$=3\times10^{-6}$/H，才能保证计算机系统的平均故障间隔时间为 10^{5} 小时。

参考答案

（1）D

试题（2）、（3）

若每一条指令都可以分解为取指、分析和执行三步。已知取指时间 $t_{\text{取指}}=4\Delta t$，分析时间 $t_{\text{分析}}=3\Delta t$，执行时间 $t_{\text{执行}}=5\Delta t$。如果按串行方式执行完 100 条指令需要__（2）__Δt。如果按照流水方式执行，执行完 100 条指令需要__（3）__Δt。

（2）A．1190　　B．1195　　C．1200　　D．1205

（3）A．504　　B．507　　C．508　　D．510

试题（2）、（3）分析

顺序执行时，每条指令都需三步才能执行完，没有重叠。总的执行时间为：

$$(4+3+5)\Delta t\times100=1200\Delta t$$

在流水线执行时，所用的时间为：

$$t_{\text{取指}}+\max\{t_{\text{分析}},t_{\text{取指}}\}+98\times\max\{t_{\text{取指}},t_{\text{分析}},t_{\text{执行}}\}+\max\{t_{\text{分析}},t_{\text{执行}}\}+t_{\text{执行}}=4\Delta t+4\Delta t+490\Delta t+5\Delta t+5\Delta t=508\Delta t$$

重叠执行时间关系为：

取指 $_k$	分析 $_k$	执行 $_k$		
	取指 $_{k+1}$	分析 $_{k+1}$	执行 $_{k+1}$	
		取指 $_{k+2}$	分析 $_{k+2}$	执行 $_{k+2}$

参考答案

（2）C （3）B

试题（4）

若内存地址区间为 4000H～43FFH，每个存贮单元可存储 16 位二进制数，该内存区域由 4 片存储器芯片构成，则构成该内存所用的存储器芯片的容量是__（4）__。

（4）A．512×16bit B．256×8bit C．256×16bit D．1024×8bit

试题（4）分析

首先将地址编码转换为十进制数，$4000H_{16}=16384_{10}$，$43FFH_{16}=7407_{10}$，然后令两个地址码相减再加 1，即得到这段地址空间中存储单元的个数，17407–16384+1=1024，因此共有 1024 个内存单元。1024×16b/4=256×16b，因此芯片的容量为 256×16b。

参考答案

（4）C

试题（5）

选择软件开发工具时，应考虑功能、__（5）__、稳健性、硬件要求和性能、服务和支持。

（5）A．易用性 B．易维护性 C．可移植性 D．可扩充性

试题（5）分析

为提高开发效率，通常的软件开发活动中需要若干开发工具的支持。而在选择这些支撑工具时，应当选择功能上满足需要、运行稳定，且具有良好服务支持的工具。另外，工具的易用性也是需要考虑的一个重要因素，因为一个容易使用的工具可有效提高开发效率。

参考答案

（5）A

试题（6）

内聚性和耦合性是度量软件模块独立性的重要准则，软件设计时应力求__（6）__。

（6）A．高内聚，高耦合 B．高内聚，低耦合

C．低内聚，高耦合 D．低内聚，低耦合

试题（6）分析

一个模块的独立度通常使用聚合和耦合程度来度量。聚合衡量模块内部各元素结合的紧密程度。耦合度量不同模块间互相依赖的程度。提高聚合程度，降低模块之间的耦合程度是模块设计应该遵循的最重要的两个原则。聚合与耦合是相辅相成的两个设计原则，模块内的高聚合往往意味着模块之间的松耦合。而要想提高模块内部的聚合性，必须减少模块之间的联系。

参考答案

（6）B

试题（7）

若某人持有盗版软件，但他本人确实不知道该软件是盗版的，则＿（7）＿承担侵权责任。

（7）A．应由该软件的持有者　　B．应由该软件的提供者

C．应由该软件的提供者和持有者共同　　D．该软件的提供者和持有者都不

试题（7）分析

“盗版软件”即侵权的软件复制品。《计算机软件保护条例》使用了软件侵权复制品持有人主观上知道或者应当知道所持软件是否为侵权复制品为标准。知道软件是侵权复制品而使用运行，持有人主观上应当属于故意，即明知故犯；有合理理由推论或者认定持有人应当知道其对所使用运行的软件为侵权复制品，如主观上存有疏忽大意等过失，而使用运行了侵权复制品，应当承担法律责任。主观上不知或者没有合理理由应知的持有人，对该软件的使用运行等行为不承担民事赔偿责任。但是当其一旦知道了所使用的软件为侵权复制品时，应当履行停止使用、销毁该软件的法律义务。

《计算机软件保护条例》第二十八条规定，软件复制品的出版者、制作者不能证明其出版、制作有合法授权的，或者软件复制品的发行者、出租者不能证明其发行、出租的复制品有合法来源的，应当承担法律责任。

参考答案

（7）B

试题（8）

＿（8）＿不属于知识产权的范围。

（8）A．地理标志权　　B．物权　　C．邻接权　　D．商业秘密权

试题（8）分析

著作权、邻接权、专利权、商标权、商业秘密权和集成电路布图设计权属于知识产权的范围。物权不属于知识产权的范围。

参考答案

（8）B

试题（9）

若文件系统容许不同用户的文件可以具有相同的文件名，则操作系统应采用＿（9）＿来实现。

（9）A．索引表　　B．索引文件　　C．指针　　D．多级目录

试题（9）分析

本题考查操作系统中文件管理的基本知识及应用。常见的目录结构有三种：一级目录结构、二级目录结构和多级目录结构。一级目录的整个目录组织是一个线性结构，在整个系统中只需建立一张目录表，系统为每个文件分配一个目录项（文件控制块）。一级目录结构简单，但缺点是查找速度慢，不允许重名及不便于实现文件共享等，因此它主

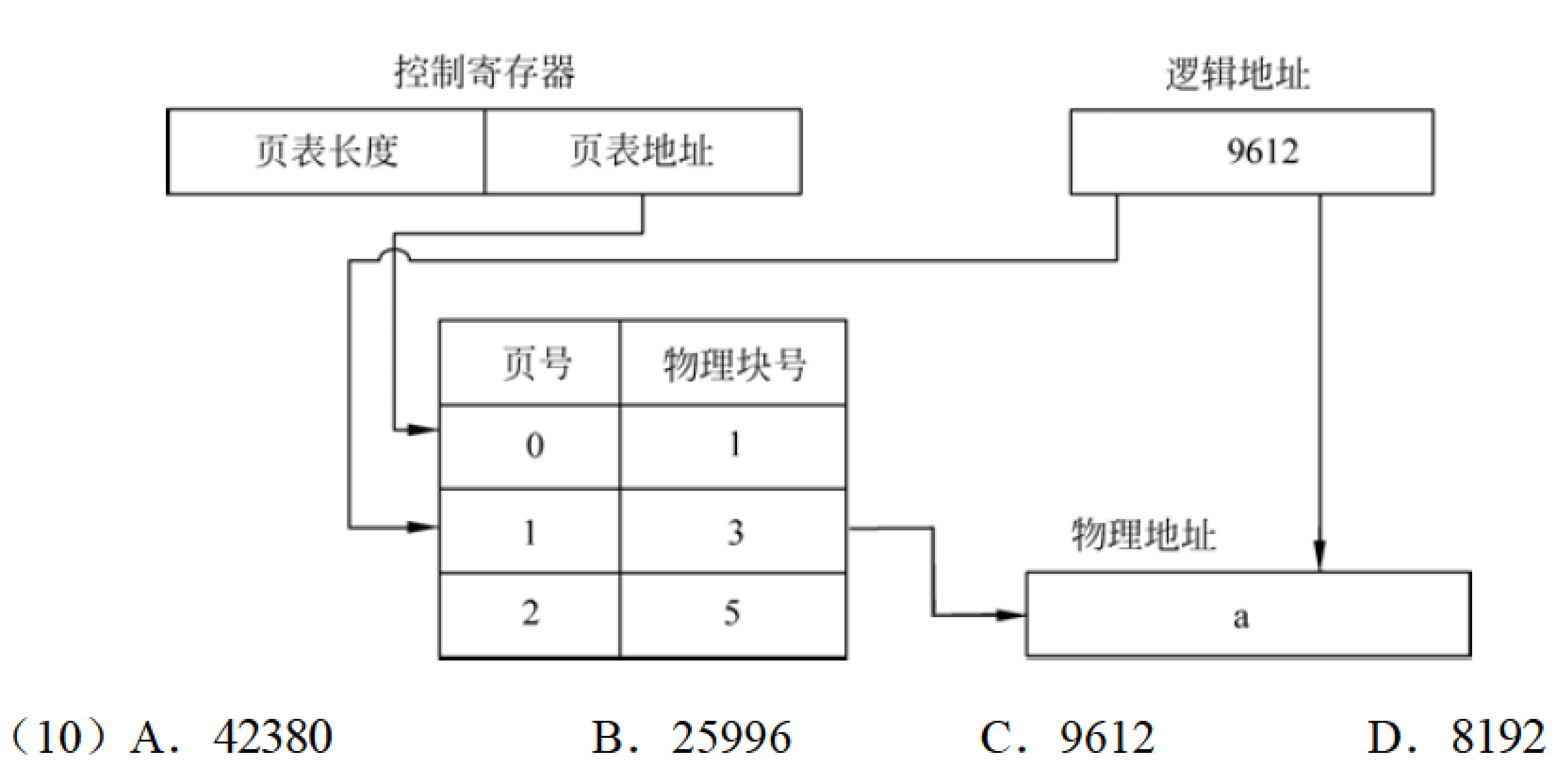
要用在单用户环境中。为了克服一级目录结构存在的缺点，引入了二级目录结构。二级目录结构是由主文件目录 MFD（Master File Directory）和用户目录 UFD（User File Directory）组成的。采用二级目录结构也存在一些问题。该结构虽然能有效地将多个用户隔离开，这种隔离在各个用户之间完全无关时是一个优点；但当多个用户之间要相互合作去共同完成一个大任务时，且一个用户又需去访问其他用户的文件时，这种隔离便成为一个缺点，因为这种隔离使诸用户之间不便于共享文件。所以引入多级目录结构，这样允许不同用户的文件可以具有相同的文件名。

参考答案

（9）D

试题（10）

页式虚拟存储系统的逻辑地址是由页号和页内地址两部分组成，地址变换过程如下图所示。假定页面的大小为 8K，图中所示的十进制逻辑地址 9612 经过地址变换后，形成的物理地址 a 应为十进制__（10）__。



（10）A．42380　　B．25996　　C．9612　　D．8192

试题（10）分析

本题考查页式存储管理中的地址变换知识。在页式存储管理中，有效地址除页的大小，取整为页号，取余为页内地址。本题页面的大小为 8KB，有效地址 9612 除 8192，取整为 1，取余为 1420。我们先查页表得物理块号 3，因此有效地址 a 为 8192×3+1420=25 996。

参考答案

（10）B

试题（11）

按照美国制定的光纤通信标准 SONET，OC-48 的线路速率是__（11）__Mb/s。

（11）A．41.84　　B．622.08　　C．2488.32　　D．9953.28

试题（11）分析

本题考查常用的数字传输系统方面的基础知识。1985 年，Bellcore 提出同步光纤网传输标准 SONET（Synchronous Optical Network）。1989 年，CCITT 参照 SONET 制定了同步数字系列标准 SDH（Synchronous Digital Hierarchy），两者有细微差别，如表 1 所示。

表 1　SONET/SDH 多路复用的速率

Optical Level	Electrical Level	Line Rate (Mbps)	Payload Rate (Mbps)	Overhead Rate (Mbps)	SDH Equivalent
OC-1	STS-1	51.840	50.112	1.728	-
OC-3	STS-3	155.520	150.336	5.184	STM-1
OC-9	STS-9	466.560	451.008	15.552	STM-3
OC-12	STS-12	622.080	601.344	20.736	STM-4
OC-18	STS-18	933.120	902.016	31.104	STM-6
OC-24	STS-24	1244.160	1202.688	41.472	STM-8
OC-36	STS-36	1866.240	1804.032	62.208	STM-13
OC-48	STS-48	2488.320	2405.376	82.944	STM-16
OC-96	STS-96	4976.640	4810.752	165.888	STM-32
OC-192	STS-192	9953.280	9621.504	331.776	STM-64

SONET/SDH 是一种通用的传输体制，不仅适于光纤，也适于微波和卫星传输，是宽带综合业务数字网（B-ISDN）的基础之一。SONET/SDH 采用 TDM 技术，是对原来应用于骨干网的准同步数字系列 PDH（Plesiochronous Digital Hierarchy）的革命。SONET 用于北美和日本，SDH 用于中国和欧洲。

参考答案

（11）C

试题（12）

关于交换机，下面说法中错误的是__（12）__。

（12）A．以太网交换机根据 MAC 地址进行交换

B．帧中继交换机根据虚电路号 DLCI 进行交换

C．三层交换机根据网络层地址进行转发，并根据 MAC 地址进行交换

D．ATM 交换机根据虚电路标识和 MAC 地址进行交换

试题（12）分析

交换机有多种，共同的特点都是根据某种标识把输入数据包交换到输出端口。以太网交换机根据 MAC 地址进行交换；帧中继交换机根据虚电路号 DLCI 进行交换；Internet 中使用的三层交换机根据 IP 地址进行转发，并根据 MAC 地址进行交换；ATM 交换机根据虚电路标识 VPI 和 VCI 进行交换。

参考答案

（12）D

试题（13）

关于路由器，下列说法中正确的是__（13）__。

（13）A．路由器处理的信息量比交换机少，因而转发速度比交换机快

B．对于同一目标，路由器只提供延迟最小的最佳路由

C．通常的路由器可以支持多种网络层协议，并提供不同协议之间的分组转换

D．路由器不但能够根据逻辑地址进行转发，而且可以根据物理地址进行转发

试题（13）分析

路由器是一种网络层转发设备，它必须分拆数据帧，识别 IP 数据报中的目标地址字段，然后进行转发。多协议路由器通常能识别多种分组格式，所以用软件实现其转发功能，处理速度比交换机慢。路由器可以实现不同的服务质量，根据 IP 报头中 ToS 字段的编码选择不同可靠性、优先级、延迟或吞吐率的线路进行转发，所以不止是提供延迟最小的路由。不但能根据逻辑地址（即 IP 地址）进行转发，而且可以根据物理地址（通常是 MAC 地址）进行交换的设备叫三层交换机。

参考答案

（13）C

试题（14）

下面关于 DPSK 调制技术的描述，正确的是__（14）__。

（14）A．不同的码元幅度不同　　B．不同的码元前沿有不同的相位改变

C．由四种相位不同的码元组成　　D．由不同的频率组成不同的码元

试题（14）分析

DPSK 是一种差分相位调制技术（Differential Phase Shift Keying），即用不同的相位变化表示数据，例如对于位 0，前沿有相位变化，对于位 1，前沿没有相位变化，如图 1 所示。

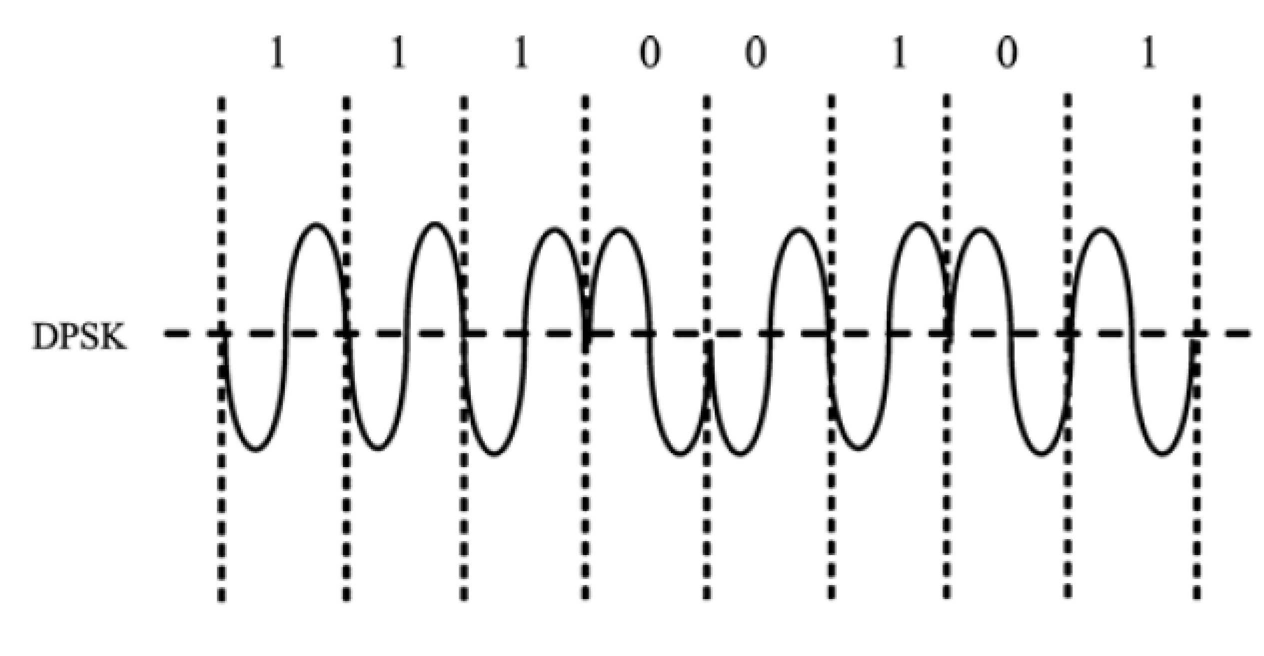


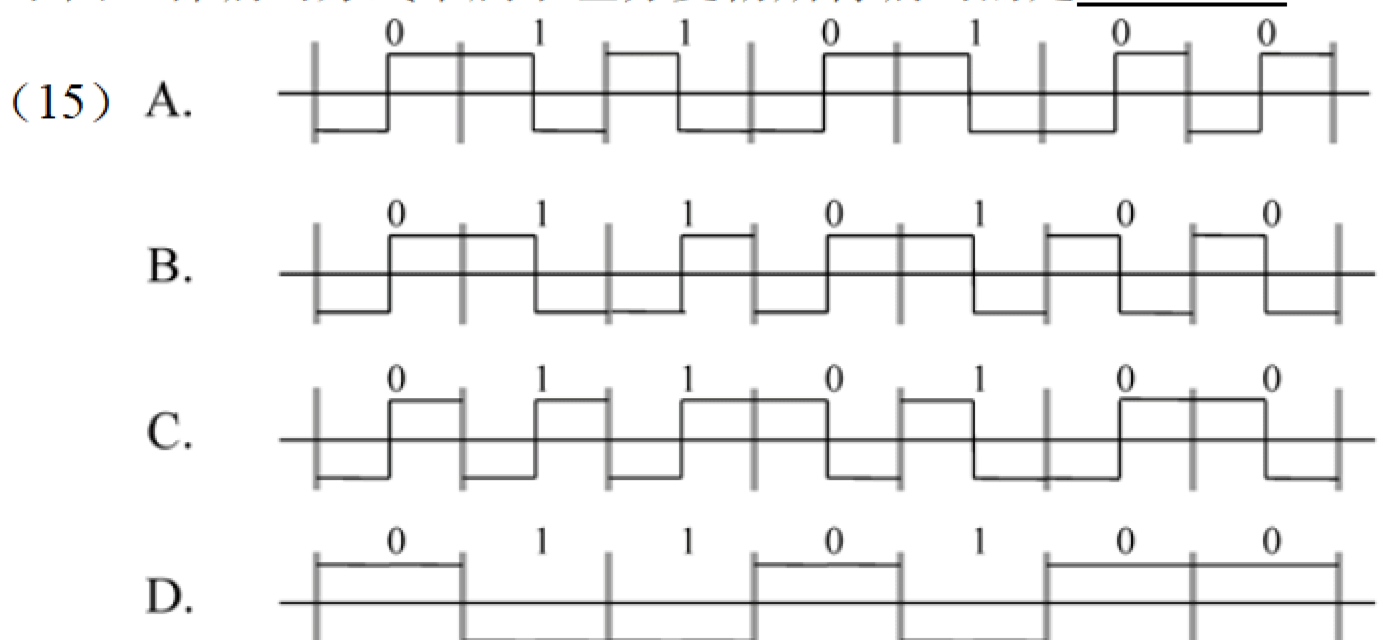
图 1　差分相位调制

参考答案

（14）B

试题（15）

下面 4 种编码方式中属于差分曼彻斯特编码的是＿（15）＿。



试题（15）分析

差分曼彻斯特编码是一种双相码。与曼彻斯特编码相同的地方是，每一位都由一正一负两个码元组成，但它又是一种差分码，0 位的前沿有相位变化，1 位的前沿没有相位变化，所以选项 B 的图形是差分曼彻斯特编码。

参考答案

（15）B

试题（16）、（17）

T1 载波每个信道的数据速率为＿（16）＿，T1 信道的总数据速率为＿（17）＿。

（16）A．32Kb/s　　B．56Kb/s　　C．64Kb/s　　D．96Kb/s

（17）A．1.544Mb/s　　B．6.312Mb/s　　C．2.048Mb/s　　D．4.096Mb/s

试题（16）、（17）分析

贝尔系统的 T1 载波（如图 2 所示）可以承载 24 路话音，每一个话音信道用 7 位表示语音编码，一位作为控制信令，24 个信道再加一个帧同步位组成一个基本帧，每个帧是 125μs，这样：

8/125μs=56Kb/s

（8×24＋1）/125μs=1.544Mb/s

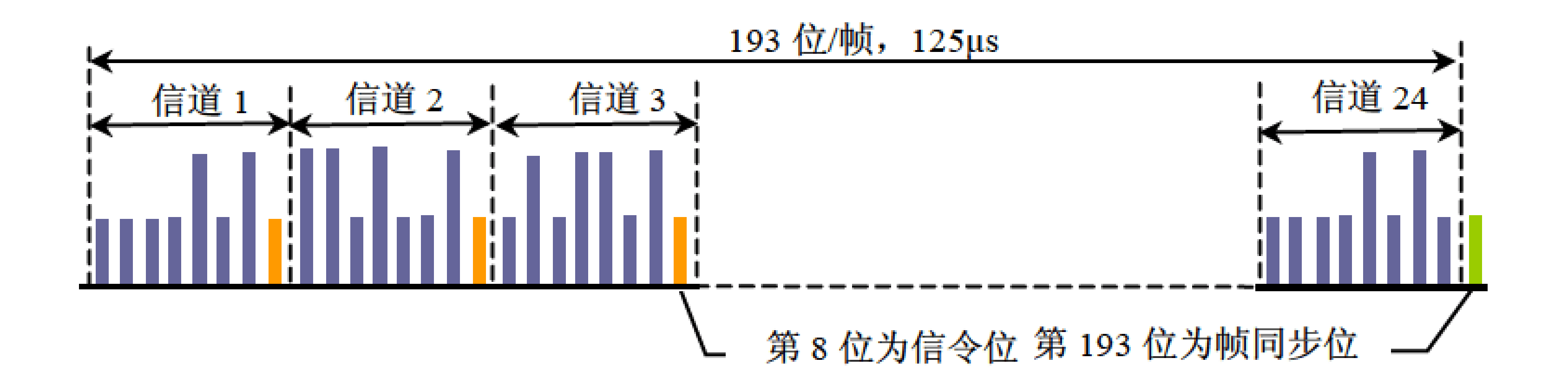


图 2　贝尔系统的 T1 载波

参考答案

（16）B （17）A

试题（18）

设信道带宽为 4000Hz，调制为 4 种不同的码元，根据 Nyquist 定理，理想信道的数据速率为__（18）__。

（18）A．10Kb/s B．16Kb/s C．24Kb/s D．48Kb/s

试题（18）分析

1924 年，贝尔实验室的研究员亨利·尼奎斯特（Harry Nyquist）推导出了有限带宽无噪声信道的极限波特率，称为“尼奎斯特定理”。若信道带宽为 W，则尼奎斯特定理指出最大码元速率为

$$B=2W\text{（Baud）}$$

按照尼奎斯特定理计算的信道容量叫做“尼奎斯特极限”，这是由信道的物理特性决定的。超过尼奎斯特极限传送脉冲信号是不可能的，所以要进一步提高波特率，必须改善信道带宽。

码元携带的信息量由码元取的离散值个数决定。若码元取两个离散值，则每个码元携带 1 位信息。若码元可取 4 种离散值，则每个码元携带 2 位信息。总之一个码元携带的信息量 n 与码元的种类数 N 有如下关系：

$$n=\log_2 N$$

单位时间内在信道上传送的信息量称为“数据速率”。在一定的波特率下提高数据速率的途径是用一个码元表示更多的位数。如果把两位编码为一个码元，则数据速率可成倍提高。公式如下

$$R=B\log_2 N=2W\log_2 N\text{（b/s）}$$

根据题中的数据，计算如下

$$R=B\log_2 N=2\times 4000\log_2 4=1600\text{b/s}=16\text{Kb/s}$$

参考答案

（18）B

试题（19）

使用 ADSL 拨号上网，需要在用户端安装__（19）__协议。

（19）A．PPP B．SLIP C．PPTP D．PPPoE

试题（19）分析

数字用户线路（Digital Subscriber Line，DSL）是以铜质电话线为传输介质的通信技术。非对称 DSL（Asymmetric DSL，ADSL）技术适用于对双向带宽要求不一样的应用，如Web浏览、多媒体点播和信息发布等。ADSL 在一对铜线上支持上行速率 640Kb/s～1Mb/s、下行速率 1Mb/s～8Mb/s，有效传输距离在 3～5 公里范围以内，支持上网冲浪的

同时还可以提供话音服务。

ADSL 接入方式分为虚拟拨号和准专线两种。采用虚拟拨号的用户需要安装 PPPoE（PPP over Ethernet）或PPPoA（PPP over ATM）客户端软件，以及类似于 Modem 的拨号程序，输入用户名称和用户密码即可连接到宽带接入站点。采用准专线方式的用户使用电信部门静态或动态分配的 IP 地址，开机即可接入 Internet。

图 3 所示为家庭个人应用的连接线路，PC 通过 ADSL Modem→分离器→入户接线盒→电话线→DSL 接入复用器（DSL Access Multiplexer，DSLAM）连接 ATM 或 IP 网络，而话音线路通过分离器→入户接线盒→电话线→DSL 接入复用器连接电话交换机。

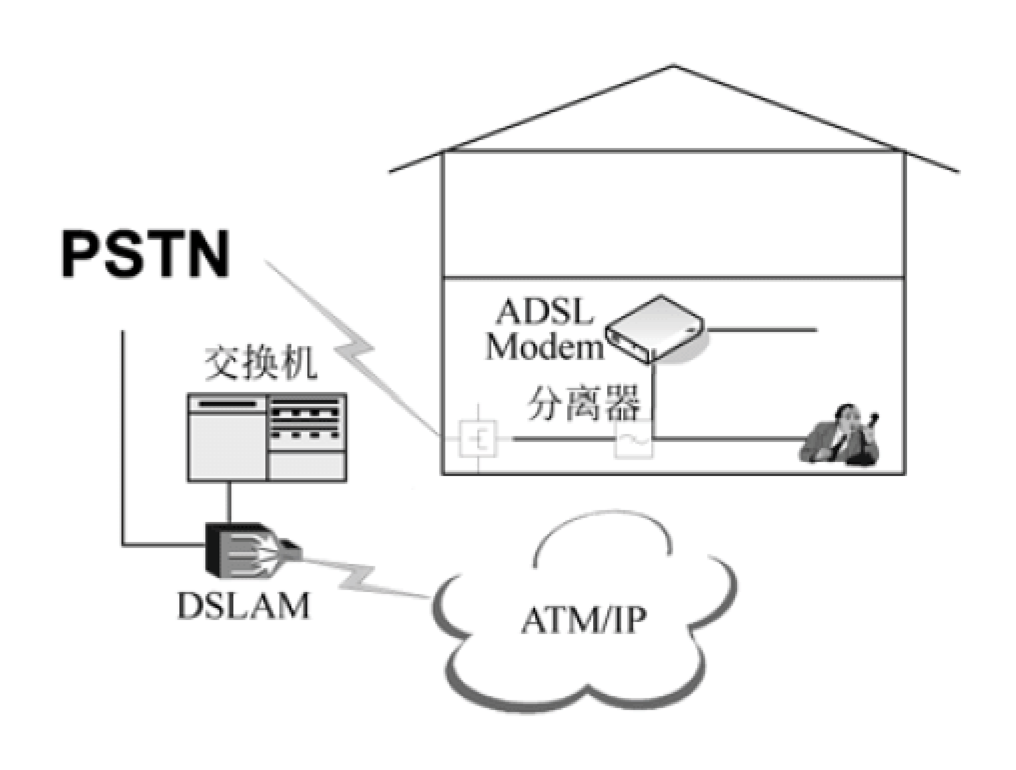


图 3　ADSL 个人应用接入

图 4 所示为企业应用的连接线路，PC 通过以太网交换机（或集线器）→ADSL 路由器→分离器→入户接线盒→电话线→DSL 接入复用器连接 ATM 或 IP 网络，而话音线路通过分离器→入户接线盒→电话线→DSL 接入复用器连接电话交换机。

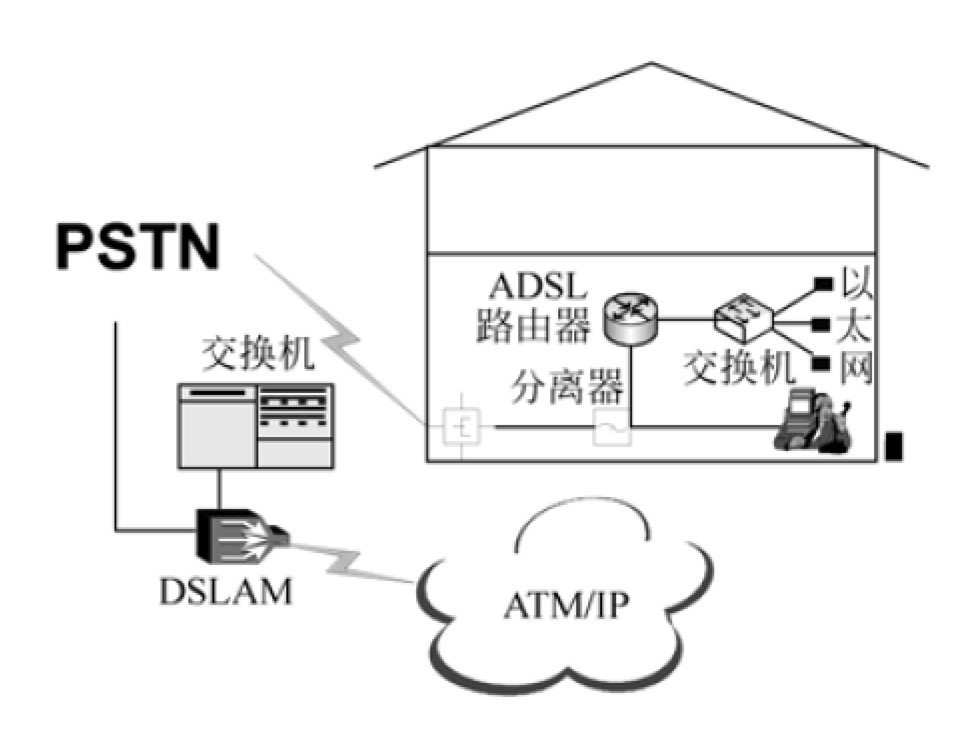


图 4　ADSL 企业应用接入

参考答案

（19）D

试题（20）

简单邮件传输协议（SMTP）默认的端口号是__（20）__。

（20）A．21 B．23 C．25 D．80

试题（20）分析

端口号是传输层协议（TCP 或 UDP）向上边的应用层提供的服务访问点。0～1023 之间的端口号固定地分配给了常见的应用。用户自己开发的应用可以在 1025～65535 之间选择端口号。简单邮件传输协议默认的端口号是 25。

参考答案

（20）C

试题（21）

在 FTP 协议中，控制连接是由__（21）__主动建立的。

（21）A．服务器端 B．客户端 C．操作系统 D．服务提供商

试题（21）分析

文件传输协议 FTP 利用 TCP 连接在客户机和服务器之间上传和下载文件。FTP 协议占用了两个 TCP 端口，FTP 服务器监听 21 号端口，准备接受用户的连接请求。当用户访问 FTP 服务器时便主动与服务器的 21 号端口建立了控制连接。如果用户要求下载文件，则必须等待服务器的 20 号端口主动发出建立数据连接的请求，文件传输完成后数据连接随之释放。在客户端看来，这种处理方式被叫做被动式 FTP，Windows 系统中默认的就是这种处理方式。由于有的防火墙阻止由外向内主动发起的连接请求，所以 FTP 数据连接可能由于防火墙的过滤而无法建立。为此有人发明了一种主动式 FTP，即数据连接也是由客户端主动请求建立的，但是在服务器中接收数据连接的就不一定是 20 号端口了。

参考答案

（21）B

试题（22）

开放最短路径优先协议（OSPF）采用__（22）__算法计算最佳路由。

（22）A．Dynamic-Search B．Bellman-Ford

C．Dijkstra D．Spanning-Tree

试题（22）分析

OSPF（RFC2328，1998）是一种链路状态协议，这种协议要求路由器掌握完整的网络拓扑结构，并据此计算出到达目标的最佳路由。OSPF 路由器通过向邻居发送一系列数据库描述分组来传送自己的数据库内容。数据库描述分组中包含了一组链路状态公告，

每个链路状态公告都描述了一条链路的状态：端口的标识和连接的目标地址。发送和接收数据库描述分组的过程叫做“数据库交换过程”。当数据库交换过程结束时，路由器之间就形成了“邻接”关系。路由更新报文在邻接的路由器之间交换，当网络拓扑发生变化时，数据库的内容随之改变。路由器利用链路状态数据库存储的信息构造有向图，并通过 Dijkstra 的最短通路优先算法（Shortest Path First，SPF）计算最小生成树，建立和更新自己的路由表。

参考答案

（22）C

试题（23）

关于 OSPF 协议，下列说法错误的是__（23）__。

（23）A．OSPF 的每个区域（Area）运行路由选择算法的一个实例

B．OSPF 路由器向各个活动端口组播 Hello 分组来发现邻居路由器

C．Hello 协议还用来选择指定路由器，每个区域选出一个指定路由器

D．OSPF 协议默认的路由更新周期为 30 秒

试题（23）分析

OSPF 是一种分层的路由协议，自治系统被划分为多个区域，每个区域运行路由选择算法的一个实例，连接多个区域的路由器运行路由选择算法的多个实例。

路由器启动时，首先初始化路由协议的数据结构并等待下层协议的指示，得到下层的工作指示后就利用 Hello 协议来发现邻居路由器。在广播网络和点对多点网络中，路由器向各个活动端口组播 Hello 分组，并接收邻居发来的 Hello 分组。所有 OSPF 路由器都准备接收目标地址为 224.0.0.5 的组播分组。

在广播网络中，Hello 协议还用来选举指定路由器。Hello 分组中包含了发送路由器的优先级，优先级最高的路由器成为指定路由器。一般来说，路由器如果从接收的 Hello 分组中发现已经存在指定路由器，它就接受这个指定路由器，而不论它自己的优先级如何。这样使得很难预计哪个路由器能够成为指定路由器，但是也使得指定路由器的改变不会太频繁。如果网络中没有指定路由器，而发送路由器的优先级最高，则它自己就成为指定路由器。

链路状态协议与距离矢量协议发布路由信息的方式不同，链路状态协议是在网络拓扑发生变化时才发布路由信息，而距离矢量协议是周期性地发布路由信息，所以链路状态协议没有固定的路由更新周期，而距离矢量协议具有设定的路由更新周期，例如 RIP 协议的路由更新周期是 30s。

参考答案

（23）D

试题（24）

在 RIP 协议中，可以采用水平分割法（Split Horizon）解决路由环路问题，下面的说法中正确的是__（24）__。

（24）A．把网络分割成不同的区域以减少路由循环

B．不要把从一个邻居学习到的路由再发送回该邻居

C．设置邻居之间的路由度量为无限大

D．路由器必须把整个路由表发送给自己的邻居

试题（24）分析

RIP 是一种距离矢量路由协议，这种算法要求相邻的路由器之间周期性地交换路由表，并通过逐步交换把路由信息扩散到网络中所有的路由器。对这种逐步交换过程如果不加以限制，将会形成路由环路（Routing Loops），使得各个路由器无法就网络的可到达性取得一致。

例如在图 5 中，路由器 A、B、C 的路由表已经收敛，每个路由表的后两项是通过交换路由信息获得的。如果在某一时刻，网络 10.4.0.0 发生故障，C 检测到故障，不再通过端口 E0 向外发送数据包，随后通过端口 S0 把故障通知 B。然而，如果 B 在收到 C 的故障通知前将其路由表发送到 C，C 会认为通过 B 可以访问 10.4.0.0，并在此基础上将路由表中第二条记录修改为（10.4.0.0，S0，2）。这样一来，路由器 A、B、C 都认为通过其他的路由器存在着一条通往 10.4.0.0 的路径，结果导致目标地址为 10.4.0.0 的数据包在三个路由器之间来回传递，从而形成路由环路。

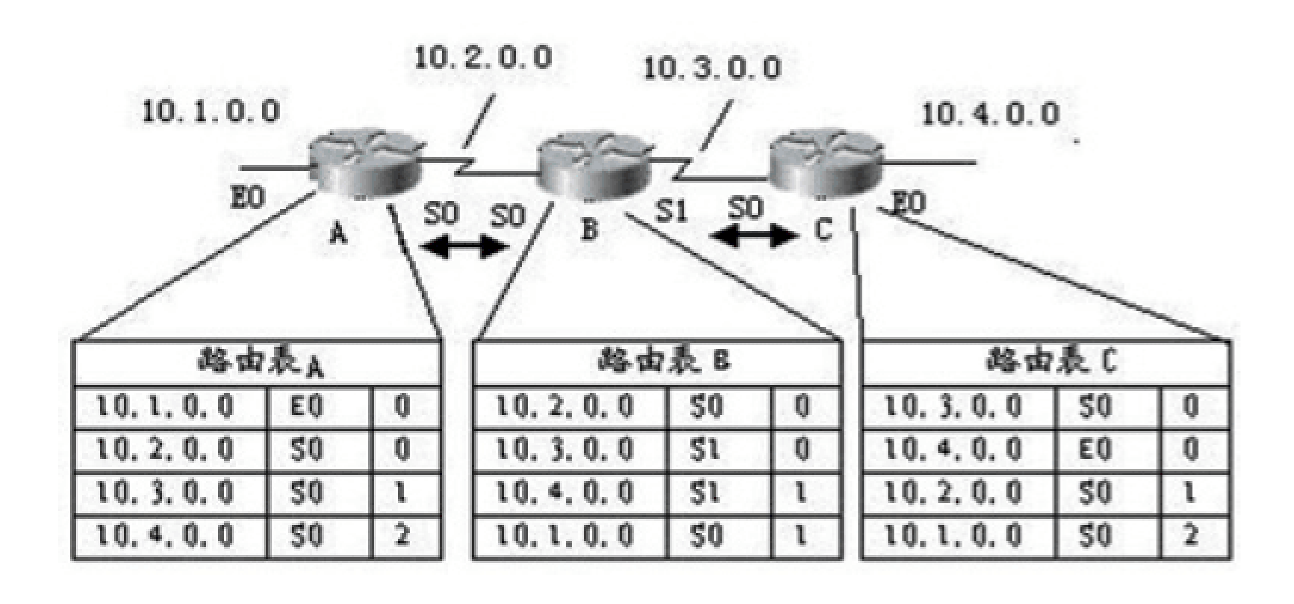


图 5　路由表

解决路由环路问题可以采用水平分割的方法。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是向邻居发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源方向。可以对图 5 中 B 的路由表项加上一些注释，如图 6 所示，可以看出，每一条路由信息都不会通过其来源端口向回发送，这样就可以避免路由环路的产生。

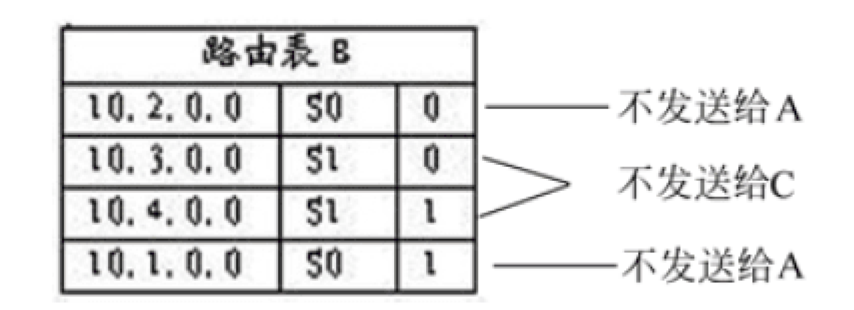


图 6　路由信息选择发送

简单的水平分割方案是，“不把从一个邻居学习到的路由发送给那个邻居”，带有反向毒化的水平分割方案（Split Horizon with Poisoned Reverse）是，“把从一个邻居学习到的路由设置为无限大，再发送给那个邻居”。采用反向毒化的方案更安全一些，它可以立即中断环路，相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成。

另外，触发更新技术也能加快路由收敛，如果触发更新足够及时——路由器 C 在接收 B 的更新报文之前把网络 10.4.0.0 的故障告诉 B，则可以防止环路的形成。

参考答案

（24）B

试题（25）

关于链路状态协议与距离矢量协议的区别，以下说法中错误的是__（25）__。

（25）A．链路状态协议周期性地发布路由信息，而距离矢量协议在网络拓扑发生变化时发布路由信息

B．链路状态协议由网络内部指定的路由器发布路由信息，而距离矢量协议的所有路由器都发布路由信息

C．链路状态协议采用组播方式发布路由信息，而距离矢量协议以广播方式发布路由信息

D．链路状态协议发布的组播报文要求应答，这种通信方式比不要求应答的广播通信可靠

试题（25）分析

链路状态协议与距离矢量协议发布路由信息的方式不同，主要有以下 4 点区别。

- 链路状态协议是在网络拓扑发生变化时才发布路由信息，而距离矢量协议是周期性地发布路由信息。
- 链路状态协议是由广播网络内部指定的路由器（Designated Router，DR）发布路由信息，而距离矢量协议的所有路由器都发布路由信息。
- 链路状态协议采用组播方式发布路由信息，而距离矢量协议则是广播路由信息。

- 链路状态协议发布的组播报文要求应答，这种通信方式比不要求应答的广播通信更可靠。

参考答案

（25）A

试题（26）

关于自治系统（Autonomous System，AS），以下说法错误的是<u>（26）</u>。

（26）A．AS 是由某一管理部门统一控制的一组网络

B．AS 的标识是唯一的 16 位编号

C．在 AS 内部采用相同的路由技术，实现统一的路由策略

D．如果一个网络要从 Internet 获取路由信息，可以使用自定义的 AS 编号

试题（26）分析

自治系统是由某一管理部门统一控制的一组网络，在 AS 内部采用相同的路由技术，实现统一的路由策略，不同 AS 采用的路由技术和路由策略可以不同。内部网关协议（Interior Gateway Protocol，IGP）用于在自治系统内部交换路由信息，例如 RIP、IGRP、EIGRP、OSPF 和 IS-IS 等都是内部网关协议。外部网关协议（Exterior Gateway Protocol，EGP）用于在两个自治系统之间交换路由信息，边界网关协议 BGP（Border Gateway Protocol）是现在唯一使用的外部网关协议。

每个自治系统被赋予唯一的 16 位编号来进行标识，因特网地址授权机构（Internet Assigned Numbers Authority，IANA）指定了地区性的注册机构，负责各个地区的号码分配，例如亚太地区归 AP-NIC（admin@apnic.net）管理。就像网络地址分为公网地址和私网地址一样，AS 编号也分为公用的和私有的两种。如果一个网络要连接到 Internet 主干网上，通过运行 BGP 协议从 Internet 获取路由信息，那么就需要向 IANA 的地区注册机构申请公用的 AS 编号。如果只是把一个内部网络划分为不同的系统，则可以使用自己定义的 AS 编号。

引入自治系统的概念可以控制网络之间路由信息的传播，例如可以选择把哪个路由器公布给其他的自治系统，也可以控制从其他自治系统中接受哪些路由器发布的信息。

参考答案

（26）D

试题（27）

TCP 段头的最小长度是<u>（27）</u>字节。

（27）A．16　　B．20　　C．24　　D．32

试题（27）分析

TCP 段头如图 7 所示，除了“任选项＋补丁”之外共有 5 行，20 个字节。

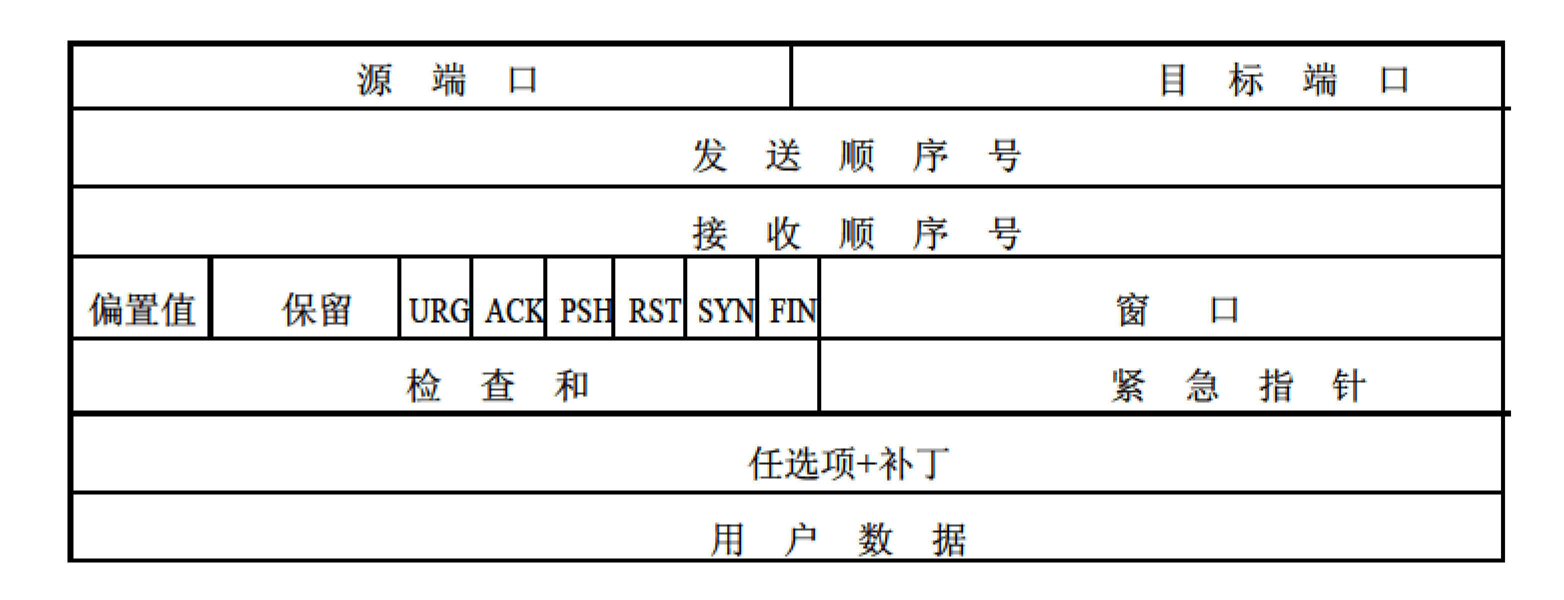


图 7　TCP 段头格式

参考答案

（27）B

试题（28）

互联网中常用的音频文件格式不包括__（28）__。

（28）A．Wave　　B．RealAudio　　C．MPEG　　D．JPEG

试题（28）分析

本题考查互联网中常用的多媒体技术的基础知识。音频文件通常分为两类：声音文件和 MIDI 文件，声音文件指的是通过声音录入设备录制的原始声音，直接记录真实声音的二进制采样数据，通常文件较大；而 MIDI 文件则是一种音乐演奏指令序列，相当于乐谱，可以利用声音输出设备或与计算机相连的电子乐器进行演奏，由于不包含声音数据，其文件尺寸较小。

Wave 格式是 Microsoft 公司开发的一种声音文件格式，用于保存 Windows 平台的音频信息资源，符合 RIFF（Resource Interchange File Format）文件规范，被 Windows 平台及其应用程序所广泛支持。它支持多种音频位数、采样频率和声道，是 PC 上最为流行的声音文件格式，但其文件尺寸较大，多用于存储简短的声音片断。

MPEG 标准中的音频部分即 MPEG 音频层（MPEG Audio Layer）。MPEG 音频文件的压缩是一种有损压缩，根据压缩质量和编码复杂程度的不同可分为三层（MPEG Audio Layer 1/2/3），分别对应 MP1、MP2 和 MP3 这三种声音文件。MPEG 音频编码具有很高的压缩率，MP1 和 MP2 的压缩率分别为 4:1 和 6:1～8:1，而 MP3 的压缩率则高达 10:1～12:1。也就是说一分钟 CD 音质的音乐，未经压缩需要 10MB 存储空间，而经过 MP3 压缩编码后只有 1MB 左右，同时其音质基本保持不失真，因此，目前使用最多的是 MP3 文件格式。

RealAudio 文件是 RealNetworks 公司开发的一种新型流式音频（Streaming Audio）文件格式，它包含在 RealNetworks 公司所制定的音频、视频压缩规范 RealMedia 中，主

要用于在低速率的广域网上实时传输音频信息。

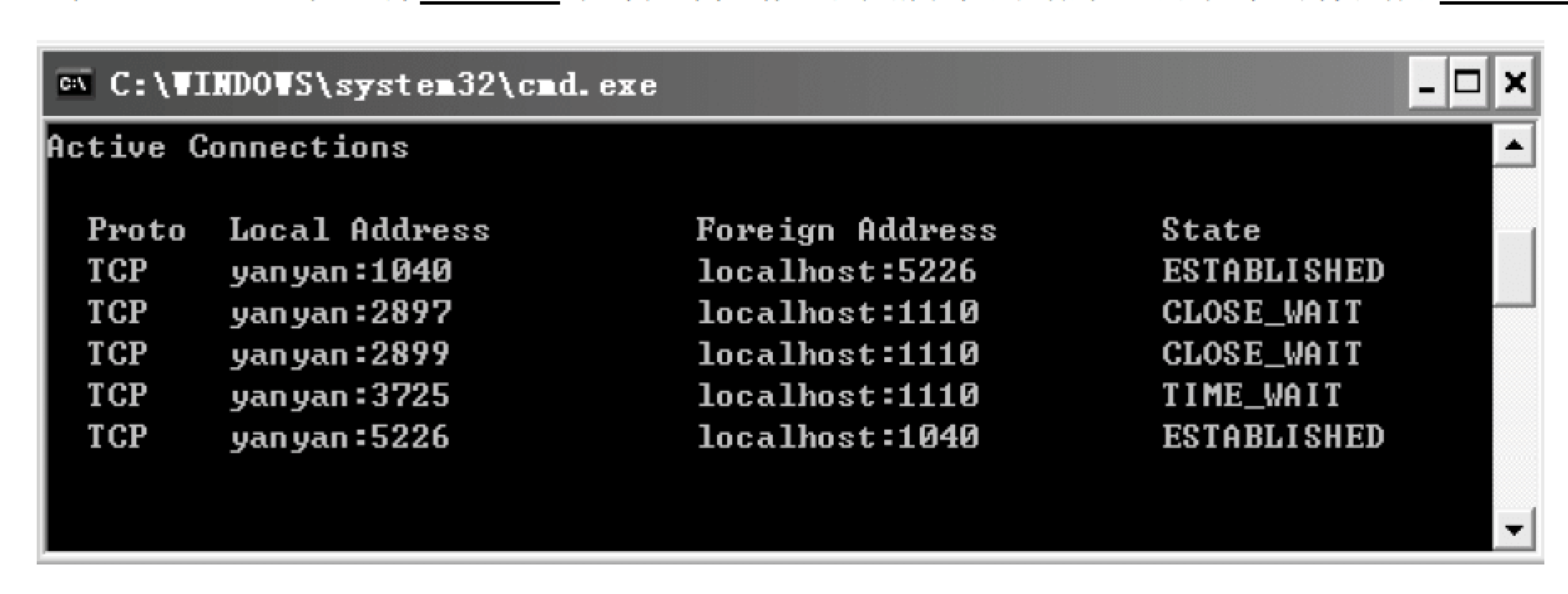
JPEG 是一种图像文件格式。ISO 和 CCITT 联合成立的“联合照片专家组”JPEG 经过 5 年艰苦细致的工作后，提出了 ISO CD 10918 号建议草案——“多灰度静止图像的数字压缩编码”（通常简称为 JPEG 标准）。这是一个适用于彩色和单色多灰度或连续色调静止数字图像的压缩标准，它包括无损压缩和基于离散余弦变换及 Huffman 编码的有损压缩两个部分。

参考答案

（28）D

试题（29）、（30）

在 Windows 中运行（29）命令后得到如下图所示的结果，该命令的作用是（30）。



（29）A. ipconfig /all　B. ping　C. netstat　D. nslookup

（30）A. 查看当前 TCP/IP 配置信息　B. 测试与目的主机的连通性
　　C. 显示当前所有连接及状态信息　D. 查看当前 DNS 服务器

试题（29）、（30）分析

ipconfig 是调试计算机网络的常用命令，通常大家使用它显示计算机中网络适配器的 IP 地址、子网掩码及默认网关。其实这只是 ipconfig 的不带参数用法，而它的带参数用法，在网络应用中也是相当不错的。其中 ipconfig/all 显示所有网络适配器（网卡、拨号连接等）的完整 TCP/IP 配置信息。与不带参数的用法相比，它的信息更全更多，如 IP 是否动态分配、显示网卡的物理地址等。

ping 是测试网络联接状况及信息包发送和接收状况非常有用的工具，是网络测试最常用的命令。Ping 向目标主机（地址）发送一个回送请求数据包，要求目标主机收到请求后给予答复，从而判断网络的响应时间和本机是否与目标主机（地址）联通。如果执行 ping 不成功，则可以预测故障出现在以下几个方面：网线故障，网络适配器配置不正确，IP 地址不正确。如果执行 ping 成功而网络仍无法使用，那么问题很可能出在网络系统的软件配置方面，ping 成功只能保证本机与目标主机间存在一条连通的物理路径。命

令格式：ping ip 地址或主机名 [-t] [-a] [-n count] [-l size]。

netstat 命令的功能是显示网络连接、路由表和网络接口信息，可以让用户得知目前都有哪些网络连接正在运作。

nslookup 最简单的用法是查询域名对应的 IP 地址，包括 A 记录、MX 记录、NS 记录和 CNAME 记录。 比如查询 A 记录：nslookup 域名。

```
C:\>nslookup www.net.cn
Server:  ns4.bta.net.cn
Address:  202.106.0.20

Non-authoritative answer:
Name:    www.net.cn
Address:  218.244.135.43
```

参考答案

（29）C　（30）C

试题（31）

要使 Samba 服务器在网上邻居中出现的主机名为 smbserver，其配置文件 smb.conf 中应包含＿（31）＿。

（31）A． workgroup=smbserver　　B． netbios name=smbserver

C． server string=smbserver　　D． guest account=smbserver

试题（31）分析

本题考查 Samba 服务器的配置知识。

在 samba 服务器配置文件 smb.conf 中，workgroup 项表示在 Windows 操作系统中的“网上邻居”中将会出现的 SAMBA 服务器所属群组，默认为 MYGROUP，不区分大小写。server string 项是 Samba 服务器的注释说明。netbios name 项定义 netbios 名字，其名字在“网上邻居”中出现。guest account 项设定访问 samba server 的来宾账户（即访问时不用输入用户名和密码的账户），若设为 pcguest 的话，则默认为 nobody 用户。

参考答案

（31）B

试题（32）、（33）

某 Apache 服务器的配置文件 httpd.conf 包含如下所示配置项。在＿（32）＿处选择合适的选项，使得用户可通过 http://www.test.cn 访问到该 Apache 服务器；当用户访问 http://111.25.4.30:80 时，会访问到＿（33）＿虚拟主机。

```
NameVirtualHost 111.25.4.30: 80
<VirtualHost 111.25.4.30: 80>
```

```
ServerName www.othertest.com
DocumentRoot /www/othertest
</VirtualHost>
<VirtualHost 111.25.4.30: 80>
ServerName  (32)
DocumentRoot /www/otherdate
</VirtualHost>
<VirtualHost 111.25.4.30: 80>
ServerName www.test.com
ServerAlias test.com *.test.com
DocumentRoot /www/test
</VirtualHost>
```

（32）A. www.othertest.com　　B. www.test.com
　　C. www.test.cn　　D. ftp.test.com

（33）A. www.othertest.com　　B. www.test.com
　　C. www.test.cn　　D. ftp.test.com

试题（32）、（33）分析

本题考查 Apache 服务器的配置。

在 Apache 服务器的配置文件 httpd.conf 中，NameVirtualHost 用来指定虚拟主机使用的 IP 地址，这个 IP 地址将对应多个 DNS 名字。如果 Apache 使用了 Listen 参数控制了多个端口，那么就可以在这里加上端口号以进一步进行区分对不同端口的不同连接请求。此后，使用 VirtualHost 语句，使用 NameVirtualHost 指定的 IP 地址作参数，对每个名字都定义对应的虚拟主机设置。

按照题目要求，用户可通过 http://www.test.cn 访问到该 Apache 服务器，而配置文件中 ServerName 缺少 www.test.cn，所以（32）处应填写 www.test.cn，当用户访问 http://111.25.4.30:80 时，会访问配置文件中定义的第一个虚拟主机 www.othertest.com。

参考答案

（32）C　（33）A

试题（34）、（35）

在配置 IIS 时，如果想禁止某些 IP 地址访问 Web 服务器，应在“默认 Web 站点”的属性对话框中＿（34）＿选项卡中进行配置。IIS 的发布目录＿（35）＿。

（34）A. 目录安全性　　B. 文档
　　C. 主目录　　D. ISAPI 筛选器

（35）A. 只能够配置在 c:\inetpub\wwwroot 上

B. 只能够配置在本地磁盘上

C. 只能够配置在联网的其他计算机上

D. 既能够配置在本地的磁盘，也能配置在联网的其他计算机上

试题（34）、（35）分析

本题考查 IIS 的配置知识。在配置 IIS 时，如果想禁止某些 IP 地址访问 Web 服务器，应在“默认 Web 站点属性”对话框中“目录安全性”选项卡的“IP 地址及域名限制”选项区域中配置。如图 8 所示。

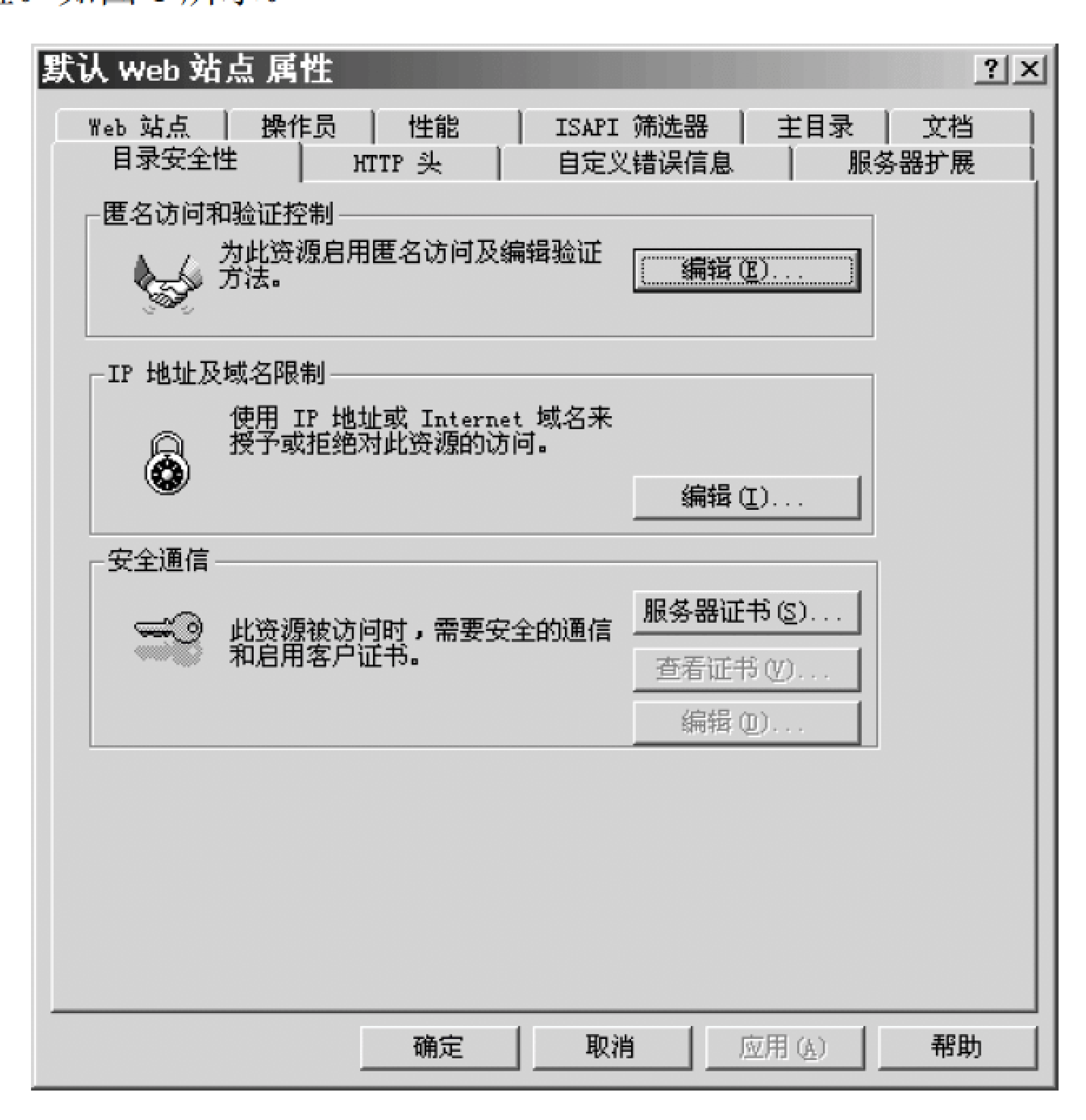


图 8　“目录安全性”选项卡

在配置 IIS 的发布目录时，可以将其配置在本机目录上、联网的其他计算机共享目录上以及重定向到 URL 上。

参考答案

（34）A　（35）D

试题（36）、（37）

活动目录（Active Directory）是由组织单元、域、__（36）__和域森林构成的层次结构，安装活动目录要求分区的文件系统为__（37）__。

（36）A. 超域　　B. 域树　　C. 团体　　D. 域控制器

（37）A. FAT16　　B. FAT32　　C. ext2　　D. NTFS

试题（36）、（37）分析

活动目录以对象的形式存储网络元素的信息，如计算机、用户等。一个对象就是一个类的实例。面向对象的存储机制保证了对象数据的安全性。Windows 的活动目录逻辑单元包括组织单元（OU）、域（Domain）、域树（Tree）和域森林（Forest），它们构成了层次的结构。域森林由域树组成，域树又由域组成，域中的对象可以按 OU 划分。OU 负责把对象组织起来。

域为活动目录的核心单元，为容器对象，它是一些基本对象（如计算机、用户等）的容器，而这些对象有相同的安全需求、复制过程和管理。活动目录中采用 DNS 域名来对域进行标记，如 reskit.com。活动目录为每个域建立一个目录数据库的副本，这个副本只存储用于这个域的对象。在域控制器之间，活动目录以多主域复制模型实现目录复制。

组织单元为一逻辑概念。由于管理上的需要，把域内的对象组织成逻辑组，如用户组、打印机组等。OU 也是一个对象的容器，用来组织、管理一个域内的对象，但 OU 不能包括来自其他域的对象。OU 可以包含各种对象，比如用户账户、用户组、计算机、打印机等，甚至可以包括其他的 OU，所以可以利用 OU 把域中的对象形成一个完全逻辑上的层次结构。

由域所组成的集合，构成域树。在域树中，每个域都拥有自己的目录数据库副本来存储自己的对象。如果从根域开始，每加入一个域，则新的域就成为树中的一个子域。域树的第一个域是该域树的根（Root），域树中的每一个域共享共同的配置、模式对象和全局目录（Global Catalog）。具有公用根域的所有域构成连续名称空间，域树上的域共享相同的 DNS 域名后缀，这就意味着子域的域名就是添加到父域域名中的那个子域的名称。

由域树所组成的集合，用信任关系相关联，共享一个公共的目录模式、配置数据和全局目录。域森林中的每一个域树具有自己唯一独立的命名空间。在域森林中创建的第一棵树默认的被创建为该域森林的根树（Root Tree）。域树和域森林的结构，可帮助活动目录使用容器层次结构来模拟一个企业的组织结构。

安装活动目录要求分区的文件系统为 NTFS。

参考答案

（36）B　（37）D

试题（38）

某 DHCP 服务器的地址池范围为 192.36.96.101～192.36.96.150，该网段下某 Windows 工作站启动后，自动获得的 IP 地址是 169.254.220.167，这是因为__（38）__。

（38）A. DHCP 服务器提供保留的 IP 地址

B．DHCP 服务器不工作

C．DHCP 服务器设置租约时间太长

D．工作站接到了网段内其他 DHCP 服务器提供的地址

试题（38）分析

本题考查 DHCP 的基本知识。本题描述中所提到的 IP 地址 169.254.220.167 实际上是自动私有 IP 地址。当 DHCP 客户端无法与 DHCP 服务器通信时，在 Windows 2000 以前的系统中，如果计算机无法获取 IP 地址，则自动配置成“IP 地址：0.0.0.0”、“子网掩码：0.0.0.0”的形式，导致其不能与其他计算机进行通信。而对于 Windows 2000 以后的操作系统，则在无法获取 IP 地址时自动配置成“IP 地址:169.254.×.×”、“子网掩码：255.255.0.0”的形式，这样可以使所有获取不到 IP 地址的计算机之间能够通信。

参考答案

（38）B

试题（39）

以下关于 FTP 和 TFTP 描述中，正确的是<u>（39）</u>。

（39）A．FTP 和 TFTP 都基于 TCP 协议

B．FTP 和 TFTP 都基于 UDP 协议

C．FTP 基于 TCP 协议，TFTP 基于 UDP 协议

D．FTP 基于 UDP 协议，TFTP 基于 TCP 协议

试题（39）分析

本题考查 FTP 的基本知识。

FTP（File Transfer Protocol，文件传输协议）是 TCP/IP 的一种具体应用，它工作在 OSI 模型的第 7 层，TCP 模型的第 4 层上，即应用层，使用 TCP 传输，FTP 连接是可靠的，而且是面向连接，为数据的传输提供了可靠的保证。

TFTP（TrivialFileTransferProtocol，简单文件传送协议）的功能与 FTP 类似，但是为了保持简单和短小，TFTP 使用UDP协议。

参考答案

（39）C

试题（40）

安全电子邮件协议 PGP 不支持<u>（40）</u>。

（40）A．确认发送者的身份　　B．确认电子邮件未被修改

C．防止非授权者阅读电子邮件　　D．压缩电子邮件大小

试题（40）分析

本题考查安全电子邮件协议 PGP 的基本知识。安全电子邮件协议 PGP（Pretty Good Privacy）在电子邮件安全实施中被广泛采用，PGP 通过单向散列算法对邮件内容进行签

名，以保证信件内容无法被修改，使用公钥和私钥技术保证邮件内容保密且不可否认。发信人与收信人的公钥都保存在公开的地方，公钥的权威性则可以由第三方进行签名认证。在 PGP 系统中，信任是双方的直接关系。

参考答案

（40）D

试题（41）

Needham-Schroeder 协议是基于__（41）__的认证协议。

（41）A. 共享密钥　B. 公钥　C. 报文摘要　D. 数字证书

试题（41）分析

本题考查有关 Needham-Schroeder 协议的基础知识。应该知道 Needham-Schroeder 协议是基于共享密钥进行认证的协议。

参考答案

（41）A

试题（42）、（43）

某 Web 网站向 CA 申请了数字证书。用户登录该网站时，通过验证__（42）__，可确认该数字证书的有效性，从而__（43）__。

（42）A. CA 的签名　B. 网站的签名　C. 会话密钥　D. DES 密码

（43）A. 向网站确认自己的身份　B. 获取访问网站的权限

C. 和网站进行双向认证　D. 验证该网站的真伪

试题（42）、（43）分析

本题考查公钥基础设施方面有关数字签名的基础知识。数字证书能够验证一个实体身份，而这是在保证数字证书本身有效性这一前提下才能够实现的。验证数字证书的有效性是通过验证颁发证书的 CA 的签名实现的。

参考答案

（42）A　（43）D

试题（44）、（45）

实现 VPN 的关键技术主要有隧道技术、加解密技术、__（44）__和身份认证技术。如果需要在传输层实现 VPN，可选的协议是__（45）__。

（44）A. 入侵检测技术　B. 病毒防治技术

C. 安全审计技术　D. 密钥管理技术

（45）A. L2TP　B. PPTP　C. TLS　D. IPSec

试题（44）、（45）分析

本题考查 VPN 方面的基础知识。应该知道实现 VPN 的关键技术主要有隧道技术、加解密技术、密钥管理技术和身份认证技术。L2TP、PPTP 是两种链路层的 VPN 协议，TLS 是传输层 VPN 协议，IPSec 是网络层 VPN 协议。

参考答案

（44）D　（45）C

试题（46）

在网络管理中要防护各种安全威胁。在 SNMPv3 中，不必要或无法防护的安全威胁是__（46）__。

（46）A．篡改管理信息：通过改变传输中的 SNMP 报文实施未经授权的管理操作

B．通信分析：第三者分析管理实体之间的通信规律，从而获取管理信息

C．假冒合法用户：未经授权的用户冒充授权用户，企图实施管理操作

D．消息泄露：SNMP 引擎之间交换的信息被第三者偷听

试题（46）分析

SNMPv3 把对网络协议的安全威胁分为主要的和次要的两类。标准规定安全模块必须提供防护的两种主要威胁如下。

- 修改信息（Modification of Information）：就是某些未经授权的实体改变了 SNMP 报文，企图实施未经授权的管理操作，或者提供虚假的管理对象。
- 假冒（Masquerade）：即未经授权的用户冒充授权用户的标识，企图实施管理操作。

标准还规定安全模块必须对两种次要威胁提供防护。

- 修改报文流（Message Stream Modification）：由于 SNMP 协议通常是基于无连接的传输服务，重新排序报文流、延迟或重放报文的威胁都可能出现。这种威胁的危害性在于通过报文流的修改可能实施非法的管理操作。
- 消息泄露（Disclosure）：SNMP 引擎之间交换的信息可能被偷听，对这种威胁的防护应采取局部的策略。

有两种威胁是安全体系结构不必防护的，因为它们不是很重要，或者这种防护没有多大作用。

- 拒绝服务（Denial of Service）：因为在很多情况下拒绝服务和网络失效是无法区别的，所以可以由网络管理协议来处理，安全子系统不必采取措施。
- 通信分析（Traffic Analysis）：即由第三者分析管理实体之间的通信规律，从而获取需要的信息。由于通常都是由少数管理站来管理整个网络的，所以管理系统的通信模式是可预见的，防护通信分析就没有多大作用了。

参考答案

（46）B

试题（47）、（48）

SNMP 协议实体发送请求和应答报文的默认端口号是__（47）__，SNMP 代理发送陷入报文（trap）的默认端口号是__（48）__。

（47）A．160　　B．161　　C．162　　D．163

（48）A．160　　B．161　　C．162　　D．163

试题（47）、（48）分析

RFC 1157 定义了 SNMP 协议的体系结构。网络管理系统由管理器（Manager）和代理（Agent）两种功能实体组成。每个被管理设备都运行一个代理进程，它的任务是收集本地的管理信息并存储在管理信息库（MIB）中；对管理器的请求给出响应，把 MIB 中有关的管理信息返回管理器；在遇到特殊情况时主动向管理器发出陷入报文。每个被管理的网络中至少有一个管理器，它的任务是收集各个被管理设备的信息，根据预定的管理策略向各个代理发出管理命令，如图 9 所示。

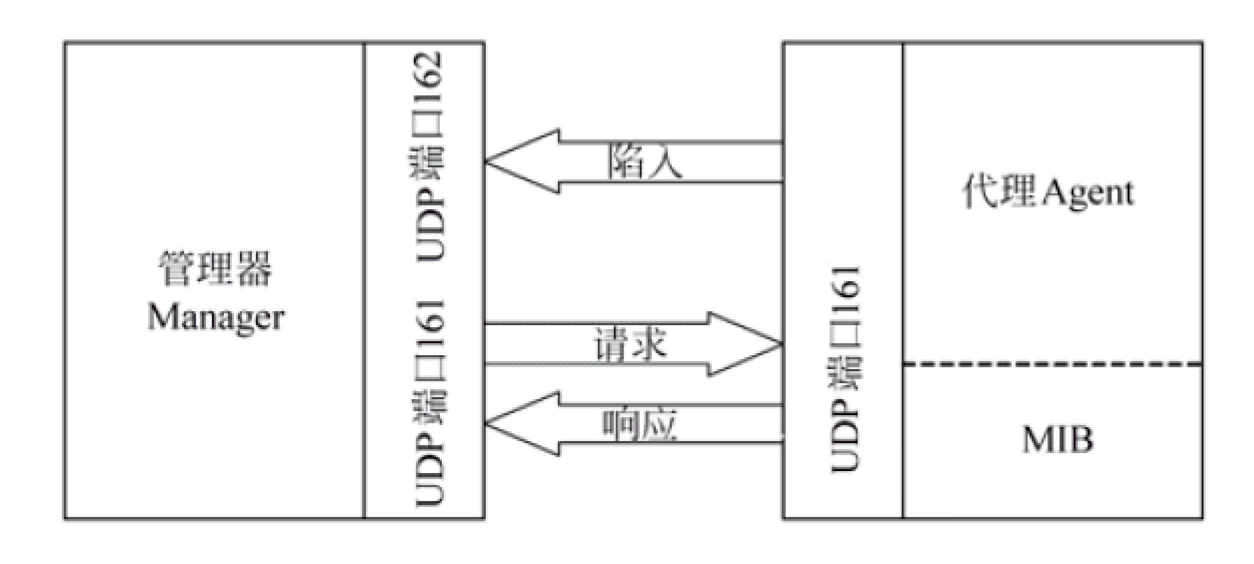


图 9　SNMP 协议的体系结构

参考答案

（47）B　（48）C

试题（49）

下面关于几个网络管理工具的描述中，错误的是__（49）__。

（49）A．netstat 可用于显示 IP、TCP、UDP、ICMP 等协议的统计数据

B．sniffer 能够使网络接口处于杂收模式，从而可截获网络上传输的分组

C．winipcfg 采用 MS-DOS 工作方式显示网络适配器和主机的有关信息

D．tracert 可以发现数据包到达目标主机所经过的路由器和到达时间

试题（49）分析

netstat（network statistics）是一个命令行工具，用于显示网络连接、路由表和网络端口收发数据包的统计信息等。

- netstat –a：显示所有连接和监听端口。
- netstat –e：显示以太网统计信息。
- netstat –n：以数字形式显示网络地址和端口号。
- netstat –r：显示路由表。
- netstat –s：按协议显示统计信息，包括 IP、ICMP、TCP 和 UDP 等。

tracert 命令的作用是跟踪数据包到达目标主机的路径，如果发现网络不通，可以用 tracert 跟踪数据包传输的路径，发现出故障的节点。例如：

```
tracert www.263.net
```

```
Tracing route to www.263.net [211.100.31.131]  （解析出 www.263.net 的主机 IP 地址）
over a maximum of 30 hops:
1 1 ms 2 ms 2 ms 202.201.3.1
2 2 ms 2 ms 2 ms 210.202.88.126
3 3 ms 4 ms 4 ms 210.112.46.13
4 5 ms 5 ms 6 ms 210.112.46.149
5 * * * Request timed out.  （从 202.112.46.149 到上一级路由器之间发生了故障）
```

winipcfg 与 ipconfig 功能一样，用于显示主机中 IP 协议的配置信息，winipcfg 适用于 Windows 95/98，而 ipconfig 适用于 Windows NT/2000/XP。winipcfg 不使用参数，它以 Windows 窗口形式显示网络适配器的物理地址、主机 IP 地址、子网掩码及默认网关等配置信息，单击其中的“其他信息”按钮，可以查看主机名、DNS 服务器和节点类型等。

sniffer 是一类程序的总称，即嗅探器，它可以通过计算机的网络接口，接收网络中传输的各种数据包，从而进行协议分析和通信流分析，解决网络维护和管理方面的问题。安装了 sniffer 的计算机，其网卡被设置为杂收（promiscuous）模式，这样就能截获网络上传输的任何数据包。与通常情况下的网卡不一样，通常的网卡默认只接收发送给自己的数据包。嗅探器可能被合法地使用，也可能被恶意地使用，网络黑客利用嗅探器程序，可以根据截获的数据包发现用户的账户信息，从而实施网络攻击活动。Sniffer（首写字母大写）是 Network General 公司开发的最早的分组捕获和代码分析软件，用于网络通信分析和故障排除。

参考答案

（49）C

试题（50）

在 Windows XP 中用事件查看器查看日志文件，可看到的日志包括__（50）__。

（50）A．用户访问日志、安全性日志和系统日志

B．应用程序日志、安全性日志和系统日志

C．网络攻击日志、安全性日志和记账日志

D．网络连接日志、安全性日志和服务日志

试题（50）分析

在桌面上单击“我的电脑”，选择右键菜单中的“管理”命令，调出计算机管理窗口，如图 10 所示。事件查看器允许用户监视“应用程序”、“安全性”和“系统”日志中记录的事件。



图 10 事件查看器

参考答案

（50）B

试题（51）

有 4 个子网：10.1.201.0/24、10.1.203.0/24、10.1.207.0/24 和 10.1.199.0/24，经路由汇聚后得到的网络地址是__（51）__。

（51）A. 10.1.192.0/20　　B. 10.1.192.0/21

C. 10.1.200.0/21　　D. 10.1.224.0/20

试题（51）分析

网络 10.1.201.0/24 的二进制表示为 **00001010 00000001 1100**1001 00000000

网络 10.1.203.0/24 的二进制表示为 **00001010 00000001 1100**1011 00000000

网络 10.1.207.0/24 的二进制表示为 **00001010 00000001 1100**1111 00000000

网络 10.1.199.0/24 的二进制表示为 **00001010 00000001 1100**0111 00000000

可以看出，按照最长匹配规则，得到的网络地址为：

10.1.192.0/20 **00001010 00000001 1100**0000 00000000

参考答案

（51）A

试题（52）

私网地址用于企业内部 IP 地址分配，网络标准规定的私网地址有__（52）__。

（52）A. A 类有 10 个：10.0.0.0～20.0.0.0

B. B 类有 16 个：172.0.0.0～172.15.0.0

C. C 类有 256 个：192.168.0.0～192.168.255.0

D. D 类有 1 个：244.0.0.0

试题（52）分析

标准规定的私网地址如下。

- 一个 A 类私网地址：10.0.0.0～10.255.255.255。
- 16 个 B 类私网地址：172.16.0.0～172.31.255.255。
- 256 个 C 类私网地址：192.168.0.0～192.168.255.255。

参考答案

（52）C

试题（53）

下面的地址中，属于本地环路地址的是（53）。

（53）A．10.10.10.1　　B．255.255.255.0
　　C．127.0.0.1　　D．192.0.0.1

试题（53）分析

用于本地环路（loopback）的 IP 地址是 127.0.0.1，通过这个地址可以检测主机 TCP/IP 协议的配置。

参考答案

（53）C

试题（54）、（55）

某校园网的地址是 202.100.192.0/18，要把该网络分成 30 个子网，则子网掩码应该是（54），每个子网可分配的主机地址数是（55）。

（54）A．255.255.200.0　　B．255.255.224.0
　　C．255.255.254.0　　D．255.255.255.0

（55）A．32　　B．64　　C．510　　D．512

试题（54）、（55）分析

把网络 202.100.192.0/18 划分成 30 个子网，需要 5 位来标识子网号，再加上原来的 18 位，则子网掩码为 255.255.254.0，还留有 9 位来表示主机地址。除过全 0 和全 1 两个地址，每个子网可分配的主机地址数为 510 个。

参考答案

（54）C　（55）C

试题（56）

在路由器的特权模式下键入命令 setup，则路由器进入（56）模式。

（56）A．用户命令状态　　B．局部配置状态
　　C．特权命令状态　　D．设置对话状态

试题（56）分析

在全局配置模式下用命令 Router#setup 进入设置对话状态（setup mode），利用设置对话状态可以避免手工输入命令的麻烦，但它不能完全代替手工配置，一些特殊的配置必须通过手工输入的方式完成。

在设置对话状态，路由器首先显示提示信息：

```
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[ ]'.
```

然后，路由器就开始全局参数的配置：

```
Configuring global parameters:
```

1．设置路由器名。

```
Enter host name [Router]:
```

2．设置进入特权状态的密钥（secret），此密钥在配置后不会以明文方式显示。

```
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.
  Enter enable secret: cisco
```

3．设置进入特权状态的口令（password），此口令只在没有密钥时起作用，并且在配置后会以明文方式显示。

```
The enable password is used when there is no enable secret
and when using older software and some boot images.
  Enter enable password: pass
```

1．设置虚拟终端访问时的口令。

```
  Enter virtual terminal password: cisco
```

2．询问是否要配置路由器支持的各种网络协议。

```
  Configure SNMP Network Management? [yes]:
  Configure DECnet? [no]:
  Configure AppleTalk? [no]:
  Configure IPX? [no]:
  Configure IP? [yes]:
  Configure IGRP routing? [yes]:
Configure RIP routing? [no]:
...
```

3．如果配置的是拨号访问服务器，系统还会配置异步端口的参数。

```
Configure Async lines? [yes]:
```

（1）配置线路的最高速度。

```
Async line speed [9600]:
```

（2）是否使用硬件流控。

```
Configure for HW flow control? [yes]:
```

（3）是否配置 Modem。

```
Configure for modems? [yes/no]: yes
```

（4）是否使用默认的 Modem 命令。

```
Configure for default chat script? [yes]:
```

（5）是否配置异步串口的 PPP 参数。

```
Configure for Dial-in IP SLIP/PPP access? [no]: yes
```

（6）是否使用动态 IP 地址。

```
Configure for Dynamic IP addresses? [yes]:
```

（7）是否使用默认 IP 地址。

```
Configure Default IP addresses? [no]: yes
```

（8）是否使用 TCP 头压缩。

```
Configure for TCP Header Compression? [yes]:
```

（9）是否在异步串口上使用路由表更新。

```
Configure for routing updates on async links? [no]: y
```

（10）是否配置异步口上的其他协议。
接下来，系统会对每个端口进行参数的设置。

```
Configuring interface Ethernet0:
```

（1）是否使用此端口。

```
Is this interface in use? [yes]:
```

（2）是否设置此端口的 IP 参数。

```
Configure IP on this interface? [yes]:
```

（3）配置端口的 IP 地址。

```
IP address for this interface: 192.168.162.2
```

（4）配置端口的 IP 子网掩码。

```
Number of bits in subnet field [0]:
Class C network is 192.168.162.0, 0 subnet bits; mask is /24
```

在配置完所有端口的参数后，系统会把整个配置对话过程的结果显示出来。

```
The following configuration command script was created:
hostname Router
enable secret 5 $1$W5Oh$p6J7tIgRMBOIKVXVG53Uh1
enable password pass
…
```

在 enable secret 后面显示的是乱码，而 enable password 后面显示的是设置的内容。显示结束后，系统问是否使用这个配置。

```
Use this configuration? [yes/no]: yes
```

如果回答 yes，系统就把配置的结果存入路由器的 NVRAM 中，然后结束设置对话状态，路由器开始正常的工作。

参考答案

（56）D

试题（57）

要进入以太端口配置模式，下面的路由器中命令，哪一条是正确的？__（57）__

（57）A. R1 (config)# interface e0　　B. R1 > interface e0

C. R1 > line e0　　D. R1 (config)# line s0

试题（57）分析

路由器的命令状态有下列几种。

1．router>

路由器处于用户命令状态，这时用户可以看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器配置的内容。

2．router#

在 router>提示符下输入 enable，路由器进入特权命令状态 router#，这时不但可以执行所有的用户命令，还可以看到和更改路由器的配置内容。

3．router(config)#

在 router#提示符下输入 configure terminal，出现提示符 router(config)#，这时路由器处于全局配置状态，可以配置路由器的全局参数。

4．router(config-if)#;

router(config-line)#;

router(config-router)#;…

路由器处于局部配置状态，这时可以配置路由器的局部参数。

5．>

在开机后 60s 内按 Ctrl+Break 键，路由器进入 RXBOOT 状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导。

要配置以太网端口，首先要进入特权命令状态，然后进入全局配置模式，最后进入局部配置模式。

参考答案

（57）A

试题（58）

要显示路由器的运行配置，下面的路由器命令中，哪一条是正确的？（58）

（58）A．R1 # show running-config　　B．R1 # show startup-config

C．R1 > show startup-config　　D．R1 > show running-config

试题（58）分析

路由器当前活动的配置文件（running-config）存储在 RAM 中，启动时的配置文件（startup-config）存储在 NVRAM 中。RAM 中存储的运行文件在关闭电源时会丢掉，必须用复制命令存储到 NVRAM 中。复制命令和显示配置文件的命令必须在特权模式下运行，在对路由器进行了简单的配置后，可以按照下面的顺序输入命令并观察结果。

```
R1#show running-config                  （显示运行文件）
Router#show startup-config              （显示启动文件）
R1#copy running-config startup-config   （复制运行文件到 NVRAM）
R1#show startup-config                  （重新显示启动文件）
R1#erase startup-config                 （删除 NVRAM 中的启动文件）
R1#show startup-config                  （显示启动文件）
R1#reload                               （重启路由器）
R1#show startup-config                  （显示启动文件）
R1#copy running-config startup-config   （复制运行文件到 NVRAM）
```

参考答案

（58）A

试题（59）

下面关于 802.1q 协议的说明中正确的是__（59）__。

（59）A. 这个协议在原来的以太帧中增加了 4 个字节的帧标记字段

B. 这个协议是 IETF 制定的

C. 这个协议在以太帧的头部增加了 26 字节的帧标记字段

D. 这个协议在帧尾部附加了 4 字节的 CRC 校验码

试题（59）分析

VLAN 帧标记有两种格式。一种是 IEEE 定义的 802.1q 协议，在原来的以太帧中增加了 4 个字节的标记（Tag）字段，如图 11 所示，其中标记控制信息（Tag ControlInformation，TCI ）包含 Priority、CFI 和 VID 三部分，各个字段的含义如表 2 所示。

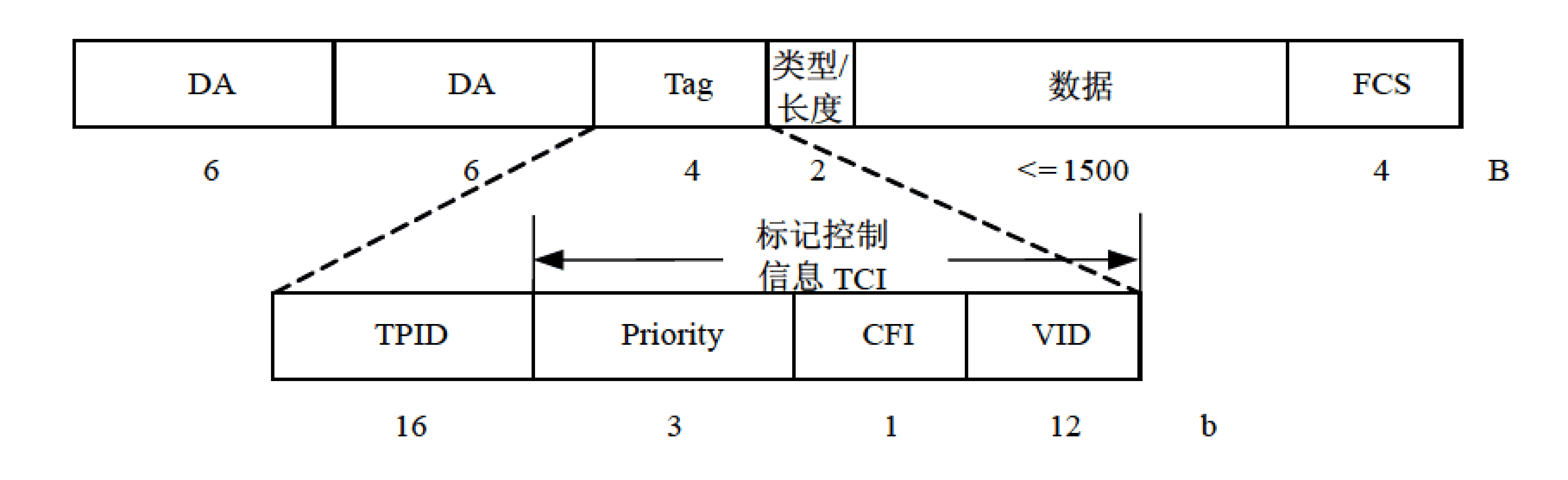


图 11 IEEE 802.1q 帧格式

表 2 802.1q 帧标记

字段	长度（b）	意 义
TPID	16	标记协议标识符（Tag Protocol Identifier），设定为 0×8100，表示该帧包含 802.1q 标记
Priority	3	提供 8 个优先级（由 802.1p 定义）。当有多个帧等待发送时，按优先级发送数据包
CFI	1	规范格式指示（Canonical Format Indicator ），0 表示以太网，1 表示 FDDI 和令牌环网。这一位在以太网与 FDDI 和令牌环网交换数据帧时使用
VID	12	VLAN 标识符（0～4095），其中 VID 0 用于识别优先级，VID 4095 保留未用，所以最多可配置 4094 个 VLAN

802.1q 并没有定义优先级的含义，提供这种功能的是 802.1p 协议。IEEE 对 8 种优先级的使用给出了一些建议：最高优先级 7 属于关键的网络通信，例如 RIP 和 OSPF 的路由更新报文；5 级和 6 级属于对网络延迟敏感的应用，例如交互式视频和语音流；1～4

级可以分配给多媒体流和关键的商业应用，或者对数据丢失敏感的应用；0 级是默认的优先级，自动被赋予"尽力而为"的网络服务。目前大部分交换机采用的交换芯片只支持两种优先级，也有的能支持 4 种优先级。

另外 802.1p 协议还提供了组播过滤机制，以配合 IP 组播功能，使得 IP 组播流量不会被交换机广播扩散。许多高档交换机都把实现 802.1p 和 802.1q 作为重要的性能指标。

另外一种帧标记是交换机间链路协议（Inter-Switch Link，ISL），ISL 协议是 Cisco 公司的专利协议，适用于 Cisco 的 Catalyst 系列交换机。ISL 协议在每个帧的头部增加 26 字节的帧标记，在帧尾部附加 4 字节的 CRC 校验码，格式如图 12（b）所示。ISL 帧标记各个字段的解释如表 3 所示。

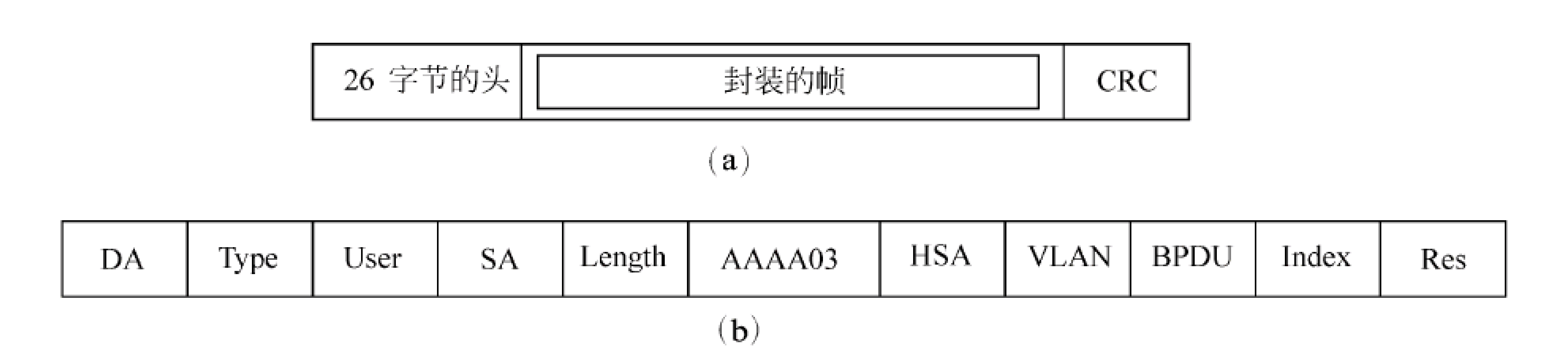


图 12　ISL 帧格式

表 3　ISL 帧标记各个字段的解释

字段	长度（b）	意　义
DA	40	目标地址，必须设置成 0X01-00-0C-00-00 或 0X03-00-0c-00-00，这 40 位是一个组播地址，通知接收器，该分组是 ISL 格式
Type	4	封装的帧类型，0000：Ethernet、0001：Token Ring、0010：FDDI、0011：ATM
User	4	帧的优先级，XX00：Normal Priority、XX01：Priority 1、XX10：Priority 2、XX11：Highest Priority
SA	48	从封装的帧中复制的源地址
Length	16	ISL 帧的总长度
AAAA03	24	常数值，指示 IEEE 802.2 LLC SNAP 帧的头部
HSA	24	源地址的高位位，必须置为 0X00-00-0c
VLAN	15	VLAN 标识符，仅使用 10 位，表示 1024 个 VLAN（0～1023）
BPDU	1	1 表示 802.1d 定义的 BPDU，0 表示 CDP 帧（Cisco Discovery Protocol）
Index	16	发送数据包的交换机端口号，用于故障诊断
Res	16	为令牌环和 FDDI 保留的字段

参考答案

（59）A

试题（60）

配置 VLAN 有多种方法，下面哪一条不是配置 VLAN 的方法？__（60）__

（60）A．把交换机端口指定给某个 VLAN

B．把 MAC 地址指定给某个 VLAN

C．由 DHCP 服务器动态地为计算机分配 VLAN

D．根据上层协议来划分 VLAN

试题（60）分析

在交换机上实现 VLAN，可以采用静态或动态的方法。

1．静态分配 VLAN：为交换机的各个端口指定所属的 VLAN。这种基于端口的划分方法是把各个端口固定地分配给不同的 VLAN，任何连接到交换机的设备都属于接入端口所在的 VLAN。如果用户改变了接入端口而又想访问原来的 VLAN，则需要为该 VLAN 增加新的端口成员。

2．动态分配 VLAN：动态 VLAN 通过诸如 Cisco Works2000 之类的软件包来创建，可以根据设备的 MAC 地址、网络层协议、网络层地址、IP 广播域或管理策略来划分 VLAN。根据 MAC 地址划分 VLAN 的方法应用最多，一般交换机都支持这种方法。无论一台设备连接到交换网络的任何地方，接入交换机通过查询 VLAN 管理策略服务器（VLAN Management Policy Server，VMPS），根据设备的 MAC 地址就可以确定该设备的 VLAN 成员身份。这种方法使得用户可以在交换网络中改变接入位置，而仍能访问所属的 VLAN，但是当用户数量很多时，对每个用户设备分配 VLAN 的工作量是很大的管理负担。

基于网络层协议划分 VLAN，需要分析各种协议的地址格式并进行相应的转换，因此需要更多的处理开销。相比利用 MAC 地址划分 VLAN，这种方法在处理速度上不占优势。

参考答案

（60）C

试题（61）

下面哪个设备可以转发不同 VLAN 之间的通信?__（61）__

（61）A．二层交换机　　B．三层交换机

C．网络集线器　　D．生成树网桥

试题（61）分析

虚拟局域网（Virtual Local Area Network，VLAN）是根据管理功能、组织机构或应用类型对交换局域网进行分段而形成的逻辑网络，其分段方法与设备的物理位置无关。虚拟局域网中的工作站可以不属于同一物理网段，属于同一个 VLAN 的所有端口构成一

个广播域，VLAN 之间的通信必须通过路由器或三层交换机进行转发。

参考答案

（61）B

试题（62）

以太网协议中使用了二进制指数后退算法，这个算法的特点是<u>（62）</u>。

（62）A. 容易实现，工作效率高

B. 在轻负载下能提高网络的利用率

C. 在重负载下能有效分解冲突

D. 在任何情况下不会发生阻塞

试题（62）分析

以太网的 MAC 子层采用 CSMA/CD 协议，当发送过程中检测到了冲突，就使用二进程指数后退算法退避一段时间后再重新试图发送。按照这种算法，后退时延的取值范围与重发次数 n 形成二进制指数关系。或者说，随着重发次数 n 的增加，后退时延 t_ξ的取值范围按 2 的指数增大。即第一次试发送时 n 的值为 0，每冲突一次，n 的值加 1，并按下式计算后退时延。

$$\begin{cases} \xi = \text{random}[0, 2^n] \\ t = \xi_\tau \end{cases}$$

其中第一式是在区间[0，2^n]中取一均匀分布的随机整数ξ，第二式是计算出随机后退时延。为了避免无限制的重发，规定当 n 增加到某一最大值（例如 16）时，放弃发送，向上层协议报告错误。二进制指数后退算法考虑了网络负载的变化情况。事实上，后退次数的多少往往与负载大小有关，二进制指数后退算法的优点是把后退时延的平均取值与负载的大小联系起来了，使得在重负载的情况下能有效地分解冲突。

参考答案

（62）C

试题（63）

以下属于万兆以太网物理层标准的是<u>（63）</u>。

（63）A. IEEE802.3u　　B. IEEE802.3a

C. IEEE802.3e　　D. IEEE802.3ae

试题（63）分析

2002 年 6 月，IEEE 802.3ae 标准发布，支持 10Gb/s 的传输速率，规定的几种传输介质如表 4 所示。传统以太网采用 CSMA/CD 协议，即带冲突检测的载波监听多路访问技术。与千兆以太网一样，万兆以太网基本应用于点到点线路，不再共享带宽，没有冲突检测，载波监听和多路访问技术也不再重要。千兆以太网和万兆以太网采用与传统以太网同样的帧结构，最大/最小帧长都不变。

表 4 IEEE 802.3ae 规定的传输介质

名 称	电 缆	最大段长	特 点
10GBase-S（Short）	50μm 的多模光纤	300m	850nm 串行
	62.5μm 的多模光纤	65m	
10GBase-L（Long）	单模光纤	10km	1310nm 串行
10GBase-E（Extended）	单模光纤	40km	1550nm 串行
10GBase-LX4	单模光纤	10km	1310nm 4×2.5Gb/s 波分多路复用（WDM）
	50μm 的多模光纤	300m	
	62.5μm 的多模光纤	300m	

参考答案

（63）D

试题（64）

快速以太网标准比原来的以太网标准的数据速率提高了 10 倍，这时它的网络跨距（最大段长） （64） 。

（64）A．没有改变　　B．变长了

C．缩短了　　D．可以根据需要设定

试题（64）分析

快速以太网标准为 IEEE 802.3u，提供的传输介质如表 5 所示。

表 5 IEEE 802.3u 规定的传输介质

名 称	电 缆	最大段长	特 点
100Base-T4	4 对 3 类 UPT	100m	3 类双绞线，8B/6T，NRZ 编码
100Base-TX	2 对 5 类 UTP，或 2 对 STP	100m	100Mb/s 全双工通信，MLT-3 编码
100Base-FX	1 对光纤	2000m	100Mb/s 全双工通信，4B/5B，NRZI 编码

与传统以太网一样，快速以太网也要考虑冲突时槽（slot）和最小帧长（Lmin）问题。快速以太网的数据速率提高了 10 倍，而最小帧长没变，所以冲突时槽缩小为 5.12μs。以太网的计算冲突时槽的公式为

$$slot \approx 2S / 0.7C + 2t_{phy}$$

其中 S 表示网络的跨距（最长传输距离），0.7C 为 0.7 倍光速（信号传播速率），t_{phy} 是发送站物理层时延，由于发送站发送和接收两次，所以取其时延的两倍值。按照上式，可得计算快速以太网跨距的计算公式

$$S \approx 0.35C(L_{\min} / R - 2t_{phy})$$

根据这个公式，当 R 变大时，网络跨距减小了。

参考答案

（64）C

试题（65）

无线局域网（WLAN）标准 IEEE 802.11g 规定的最大数据速率是__（65）__。

（65）A．1Mb/s　　B．11Mb/s　　C．5Mb/s　　D．54Mb/s

试题（65）分析

目前的 WLAN 标准主要有 4 种，如表 6 所示。

表 6　IEEE 802.11 标准

名　称	发布时间	工作频段	调制技术	数 据 速 率
802.11	1997 年	2.4GHz ISM 频段	DBPSK DQPSK	1Mb/s 2Mb/s
802.11b	1998 年	2.4GHz ISM 频段	CCK	5.5Mb/s，11Mb/s
802.11a	1999 年	5GHz U-NII 频段	OFDM	54Mb/s
802.11g	2003 年	2.4GHz ISM 频段	OFDM	54Mb/s

IEEE 802.11g 标准与 802.11b 都使用了 2.4GHz 的 ISM 频段，两者可以共存在同一 AP 的网络里，有利于原来的 WLAN 向高速网络过渡，降低了投资费用。

参考答案

（65）D

试题（66）

无线局域网标准 IEEE 802.11i 提出了新的 TKIP 协议来解决__（66）__中存在的安全隐患。

（66）A．WAP 协议　　B．WEP 协议　　C．MD5　　D．无线路由器

试题（66）分析

IEEE 802.11i 在 2004 年 6 月成为正式标准，作为 802.11 家族的一部分，802.11i 为 802.11a、802.11b 和 802.11g 无线局域网提供了全新的安全技术。802.11i 定义了新的密钥交换协议 TKIP（Temporal Key Integrity Protocol）和高级加密标准 AES（Advanced Encryption Standard）。TKIP 是对 WEP（Wired Equivalency Protocol）协议的改进，它提供了报文完整性检查，每个数据包使用不同的混合密钥（per-packet key mixing），每次建立连接时生成一个新的基本密钥（re-keying），这些手段的采用使得诸如密钥共享、碰撞攻击和重放攻击等无能为力，从而弥补了 WEP 协议的安全隐患。

参考答案

（66）B

试题（67）

采用以太网链路聚合技术将__（67）__。

（67）A．多个逻辑链路组成一个物理链路　B．多个逻辑链路组成一个逻辑链路
C．多个物理链路组成一个物理链路　D．多个物理链路组成一个逻辑链路

试题（67）分析

本题考查链路聚合技术。链路聚合是将两个或更多数据物理信道结合成一个单个的信道，该信道以一个单个的更高带宽的逻辑链路出现。链路聚合一般用来连接一个或多个带宽需求大的设备，例如连接骨干网络的服务器或服务器群。如果聚合的每个链路都遵循不同的物理路径，则聚合链路也提供冗余和容错。通过聚合调制解调器链路或者数字线路，链路聚合可用于改善对公共网络的访问。链路聚合也可用于企业网络，以便在吉比特以太网交换机之间构建多吉比特的主干链路。

参考答案

（67）D

试题（68）

在冗余磁盘阵列中，以下不具有容错技术的是__（68）__。

（68）A．RAID 0　B．RAID 1　C．RAID 3　D．RAID 5

试题（68）分析

本题考查冗余磁盘阵列的基本知识。RAID 0 把 n 块同样的硬盘用硬件的形式通过智能磁盘控制器或用操作系统中的磁盘驱动程序以软件的方式串联在一起，形成一个独立的逻辑驱动器，容量是单独硬盘的 n 倍。在计算机数据写时被依次写入到各磁盘中，当一块磁盘的空间用尽时，数据就会被自动写入到下一块磁盘中。它的好处是可以增加磁盘的容量。速度与其中任何一块磁盘的速度相同，如果其中的任何一块磁盘出现故障，整个系统将会受到破坏，可靠性是单独使用一块硬盘的 1/n。

RAID 1 称为磁盘镜像，把一个磁盘的数据镜像到另一个磁盘上，在不影响性能情况下最大限度地保证系统的可靠性和可修复性上，具有很高的数据冗余能力。但磁盘利用率为 50%，故成本最高，多用在保存关键性重要数据的场合。

RAID 3 使用一个专门的磁盘存放所有的校验数据，而在剩余的磁盘中创建带区集分散数据的读写操作。

RAID 5 把校验块分散到所有的数据盘中。RAID 5 使用了一种特殊的算法，可以计算出任何一个带区校验块的存放位置。这样就可以确保任何对校验块进行的读写操作都会在所有的 RAID 磁盘中进行均衡，从而消除了产生瓶颈的可能。

参考答案

（68）A

试题（69）、（70）

在进行金融业务系统的网络设计时，应该优先考虑__（69）__原则。在进行企业网络的需求分析时，应该首先进行__（70）__。

（69）A．先进性　　B．开放性　　C．经济性　　D．高可用性

（70）A．企业应用分析　　B．网络流量分析

C．外部通信环境调研　　D．数据流向图分析

试题（69）、（70）分析

网络设计一般要遵循如下一些原则。

- 先进性：建设一个现代化的网络系统，应尽可能采用先进而成熟的技术，应在一段时间内保证其主流地位。但是太新的技术也有不足之处，一是有可能不成熟，二是标准可能还不完备、不统一，三是价格高，四是可能技术支持力量不够。
- 开放性：采用国际通用的标准和技术获得良好的开放性，是网络互连互通的基础。
- 经济性：在满足需求的基础上，应该尽量节省费用。
- 高可用性：系统要有很高的平均无故障时间和尽可能低的平均故障率，一般需要采取热备份、冗余等技术。

金融系统涉及银行、众多储户的资产信息，数据重要、敏感，数据量庞大，必须要保证数据的绝对安全，同时要保证系统小的响应时间、很高的服务成功率，而且服务要完整、不间断，故障恢复能力强，整个系统要具有非常高的可用性和可靠性，并不追求采用先进的技术。另外，一般金融系统都是封闭运行的，开放性也不需要放在优先考虑的地位。因此在进行有关金融系统的网络设计时，高可用性是首要考虑的原则。

在进行企业网络的需求分析时应该首先进行企业的业务和应用分析，因为网络建设是企业应用的基础，网络系统要向企业的应用系统提供良好的服务，企业的应用需求是设计网络系统的重要依据。

参考答案

（69）D　（70）A

试题（71）～（75）

Traditional Internet access methods like dial-up were so slow that host computers were connected to the dial-up __（71）__ at the customer premise over slow __（72）__ ports. PPP was designed to run directly over these serial links. But with the advent of broadband Internet __（73）__ technologies such as ADSL and cable modems there has been a considerable increase in the bandwidth delivered to the end users. This means that the host computers at the customer premise connect to the __（74）__ or cable "modem" over a much faster medium such as Ethernet. It also means that multiple __（75）__ can connect to the Internet through the same

connection.

（71）A．buffer B．modem C．computer D．server

（72）A．parallel B．digital C．serial D．variable

（73）A．access B．cache C．cast D．storage

（74）A．FDDI B．HDSL C．ADSL D．CDMA

（75）A．cables B．hosts C．servers D．modems

参考译文

传统的 Internet 接入方法（例如拨号接入）速度很慢，这种方式要求客户端主机通过低速串口连接到拨号 Modem，在串行链路上运行 PPP 协议。但是随着宽带 Internet 接入技术——例如 ADSL 和线缆调制解调器的发展，提供给端用户的带宽已经有相当大的增加。这意味着客户端主机可以连接到 ADSL 或者线缆调制解调器，从而获得比以太网还要快得多的传输介质。这也意味着多个主机可以通过同一连接访问 Internet。

参考答案

（71）B （72）C （73）A （74）C （75）B

第 14 章　2007 下半年网络工程师下午试题分析与解答

试题一（15 分）

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

某校园网物理地点分布如图 1-1 所示，拓扑结构如图 1-2 所示：

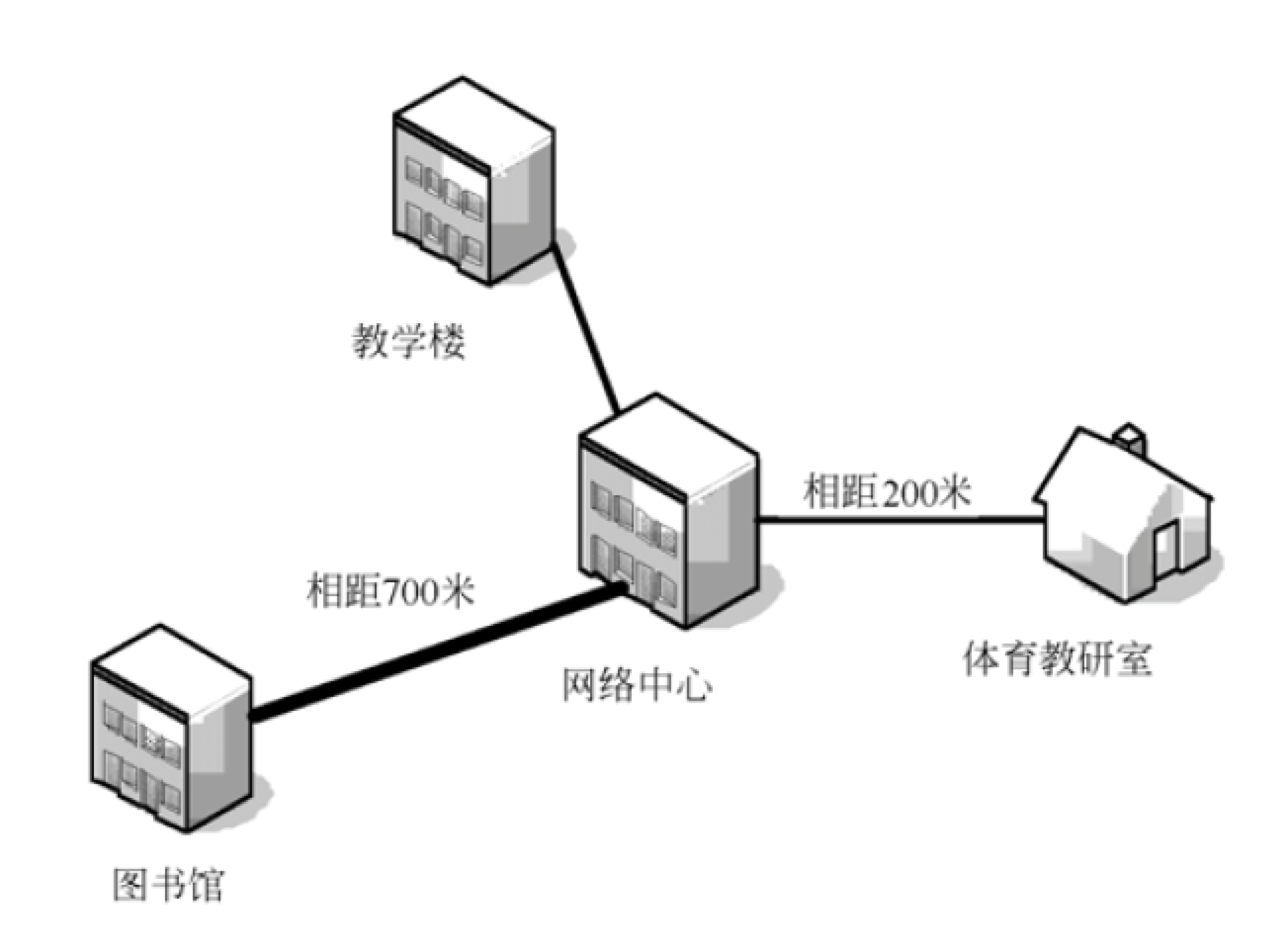


图 1-1

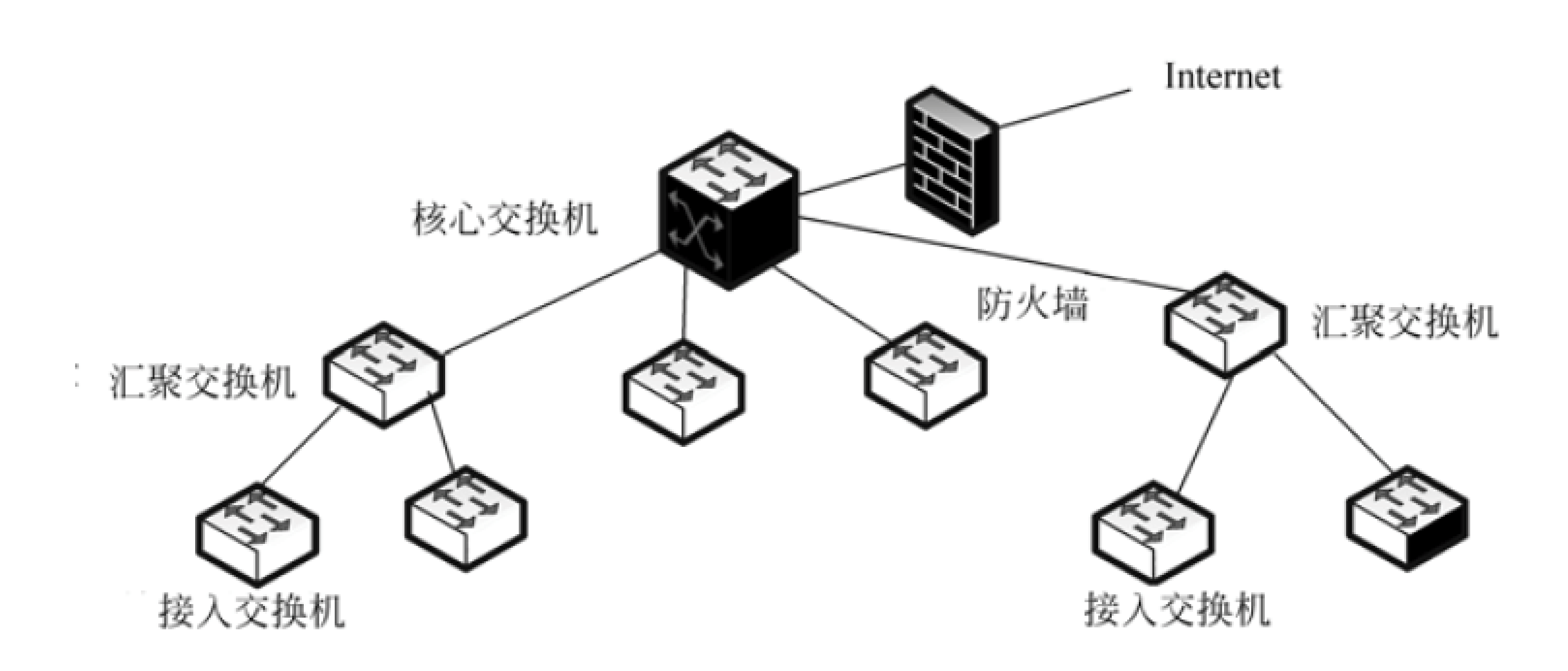


图 1-2

【问题 1】

由图 1-1 可见，网络中心与图书馆相距 700 米，而且两者之间采用千兆连接，那么两个楼之间的通信介质应选择__(1)__，理由是__(2)__。

备选答案：

（1）A．单模光纤　B．多模光纤　C．同轴电缆　D．双绞线

【问题 2】

校园网对校内提供 VOD 服务，对外提供 Web 服务，同时进行网络流量监控。对以上服务器进行部署：VOD 服务器部署在__(3)__；Web 服务器部署在__(4)__；网络流量监控服务器部署在__(5)__。

（3）（4）（5）的备选答案：

A．核心交换机端口　B．核心交换机镜像端口　C．汇聚交换机端口

D．接入交换机端口　E．防火墙 DMZ 端口

以上三种服务器中通常发出数据流量最大的是__(6)__。

【问题 3】

校园网在进行 IP 地址部署时，给某基层单位分配了一个 C 类地址块 192.168.110.0/24，该单位的计算机数量分布如表 1-1 所示。要求各部门处于不同的网段，请将表 1-2 中的（7）～（14）处空缺的主机地址（或范围）和子网掩码填写在答题纸的相应位置。

表 1-1

部　门	主机数量
教师机房	100 台
教研室 A	32 台
教研室 B	20 台
教研室 C	25 台

表 1-2

部　门	可分配的地址范围	子网掩码
教师机房	192.168.110.1～（7）	（11）
教研室 A	（8）	（12）
教研室 B	（9）	（13）
教研室 C	（10）	（14）

试题一分析

本题考查的是计算机网络部署的基本知识，包括通信介质选择、服务器部署和 IP 地址分配。

【问题 1】

按照千兆以太网的规范，使用双绞线其传输距离是中间的线缆长度＋两端的跳线长度不能超过 100m；同轴电缆在千兆传输时能够达到 25m 的距离；而多模光纤，千兆数据通信的距离规范为 220m～550m，其中当使用的光纤核心直径是 62.5μm 时，通信距离为 220m，光纤核心直径是 50μm 时，通信距离为 550m；对于单模光纤而言，在千兆传输时最大连接距离可达 5 公里。按照题目要求网络中心与图书馆相距 700m，而且两者之间采用千兆连接，那么两个楼之间的通信介质应选择单模光纤。

【问题 2】

服务器在进行部署时应充分考虑到功能，服务提供对象，流量和安全等因素。按照题目要求，VOD 服务对校内提供服务，且其流量较大，应部署在核心交换机端口。而 Web 服务器需对外提供服务，一般部署在防火墙 DMZ 端口。网络流量监控需要监听交换网络中所有流量，但是通过普通交换机端口去获取这些流量有相当大的困难，因此需要通过配置交换机来把一个或多个端口（VLAN）的数据转发到某一个端口来实现对网络的监听，这个端口就是镜像端口，而网络流量监控服务器需要部署在镜像端口。

【问题 3】

在进行 IP 地址部署时，由于要求各部门处于不同的网段，这样就要求在给定的网段内划分地址。有题目可知，教师机房起始地址为 192.168.110.1，主机数量为 100 台，因此其子网掩码为 255.255.255.128，可用地址为 192.168.110.1～192.168.110.126；教研室 A 分配的 IP 地址不能少于 32 个可用地址，因此其子网掩码为 255.255.255.192；教研室 B、教研室 C 可用地址不能少于 20 和 25，因此其子网掩码为 255.255.255.224。其中，只有教师机房的起始地址固定，其他的可组合分配。

参考答案

【问题 1】

（1）A 或单模光纤

（2）要点：传输速率千兆，距离超过 550m

【问题 2】

（3）A 或核心交换机端口　　（4）E 或防火墙 DMZ 端口

（5）B 或核心交换机镜像端口　　（6）VOD 服务器

【问题 3】

（7）192.168.110.126

（8）～（10）正确答案有 4 种组合，每种组合均正确。

组合 1：

（8）192.168.110.129～192.168.110.190

（9）192.168.110.193～192.168.110.222

（10）192.168.110.225～192.168.110.254

组合 2：

（8）192.168.110.129～192.168.110.190

（9）192.168.110.225～192.168.110.254
（10）192.168.110.193～192.168.110.222

组合 3：

（8）192.168.110.193～192.168.110.254
（9）192.168.110.129～192.168.110.158
（10）192.168.110.161～192.168.110.190

组合 4：

（8）192.168.110.193～192.168.110.254
（9）192.168.110.161～192.168.110.190
（10）192.168.110.129～192.168.110.158
（11）255.255.255.128
（12）255.255.255.192
（13）255.255.255.224
（14）255.255.255.224

试题二（15 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

网络工程师经常会面对服务器性能不足的问题，尤其是网络系统中的核心资源服务器，其数据流量和计算强度之大，使得单一计算机无法承担。可以部署多台 Linux 服务器组成服务器集群，采用负载均衡技术提供服务。

某企业内部网（网络域名为 test.com）由三台 Linux 服务器提供服务，其中 DNS、FTP、SMTP 和 POP3 四种服务由一台服务器承担，Web 服务由两台 Linux 服务器采用负载均衡技术承担。

【问题 1】

假定提供 Web 服务的两台 Linux 服务器 IP 地址分别为 192.168.1.10 和 192.168.1.20。为了使用 DNS 循环机制，由主机名 www.test.com 对外提供一致的服务，需要在 DNS 服务器的 test.com 区域文件中增加下列内容：

www1 IN <u>（1）</u> 192.168.1.10
www2 IN <u>（1）</u> 192.168.1.20
www IN <u>（2）</u> www1
www IN <u>（2）</u> www2

通过 DNS 的循环机制，客户访问主机 www.test.com 时，会依次访问 IP 地址为 192.168.1.10 和 192.168.1.20 的 www 主机。填写上面的空格，完成 test.com 文件的配置。

【问题 2】

采用循环 DNS 配置可以实现简单的具有负载均衡功能的 Web 服务。说明采用循环 DNS 实现均衡负载存在什么问题。

【问题 3】

图 2-1 所示的是基于硬件的负载均衡方案，其中 WSD Pro 被称为导向器，通过导向器的调度，实现服务的负载均衡。主机 www1.test.com、www2.test.com、ns.test.com 和 WSD Pro 都配置了双网卡，IP 地址标注在图中。

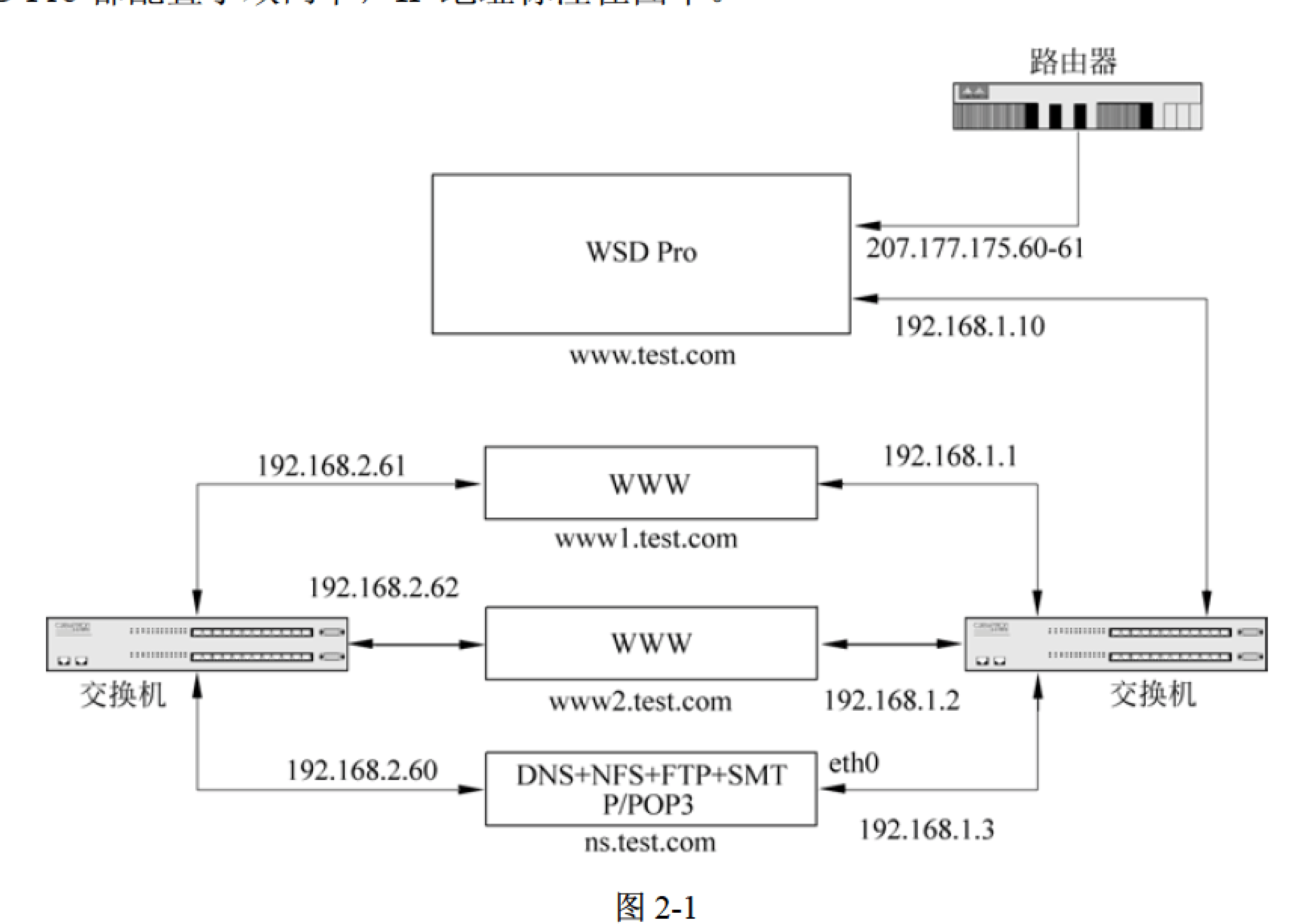


图 2-1

图中的各个服务器必须进行恰当的配置，主机 ns.test.com 的/etc/sysconfig/network 文件和/etc/sysconfig/network-scripts/ifcfg-eth0 文件配置如下：

```
/etc/sysconfig/network 文件清单：
NETWORKING=yes
FORWARD_IPV4=（3）
HOSTNAME=ns.test.com
DOMAINNAME=（4）
GATEWAY=（5）
GATEWAYDEV=eth0
/etc/sysconfig/network-scripts/ifcfg-eth0 文件清单：
DEVICE=eth0
IPADDR=（6）
NETMASK=255.255.255.0
NETWORK=（7）
BROADCAST=（8）
ONBOOT=yes
```

填写上面的空格，完成文件的配置。

【问题 4】

图 2-1 所示案例采用 NFS（网络文件系统）技术主要解决什么问题？由图中左边的交换机组成的局域网有何功能？

试题二分析

采用多个服务器组成“集群”不仅能够提高整个系统的可靠性，而且还能够分担系统负载（负载均衡）。

应用循环 DNS 配置技术可以实现不能动态调整的、简单的负载均衡技术，具体来讲就是通过恰当配置 DNS 区域文件，将两台不同 IP 地址的服务器，利用“别名”机制关联到一个统一的主机名上，客户通过这个统一的主机名访问服务器资源时，DNS 名称服务器将依次给出第一个服务器的 IP 地址、第二个服务器的 IP 地址、第一个服务器的 IP 地址……，不间断地循环。循环 DNS 配置的缺点之一是，名称服务器没有办法知道哪台服务器负载重，如果一台服务器崩溃或由于某种原因不可用了，循环 DNS 仍将返回不可用的服务器的 IP 地址，使有些用户能够访问成功而有些用户访问不成功。

采用基于硬件（导向器）的负载均衡方法能够克服上述缺点。图中 WSD Pro 导向器拦截了所有访问服务器资源的通信连接，根据一种或多种算法选择一台服务器（物理上的）将连接进行转发，比如导向器可以根据服务器的“忙碌”情况来选择，即导向器可以利用网络和服务的可用性及服务器的性能来选择某个服务器向客户提供服务。

采用上述方法实施负载均衡还需要解决服务器之间的数据同步等关键问题，必须要有另外一种机制来保证不同的服务器对外提供的服务是一致的。在第三台服务器上（本题中是 DNS 服务器）安装 NFS 系统是可行的解决方案，可在该服务器上一个或多个磁盘中安装，Web 服务器通过 NFS 可以共享访问这些磁盘。但是应该看到，采用这种方法工作效率会较低，而且存在单点故障。实际应用时，NFS 系统仅共享小的文件系统，其他数据通过某种机制（如 rdist）向 Web 服务器分发以保证数据资源一致，当然这个问题不在本试题考试范围之中。

题图中所示的实际解决方案包括两个局域网，右边的局域网通过导向器对外提供网络服务，左边的局域网称为 NFS 专用局域网，用于服务器之间的数据共享和同步，两个局域网互相独立，不能互相访问，互不干扰。因此名字服务器上的双网卡（处于两个不同的局域网）之间不能转发 IP 包，其配置文件中的 FORWARD_IPV4 应设置为 0（或 no）。

NFS 服务器的 eth0 网卡的地址是 192.168.1.3，其/etc/sysconfig/network 文件内容如下：

```
NETWORKING=yes
FORWARD_IPV4=0
HOSTNAME=ns.test.com
DOMAINNAME=test.com
```

```
GATEWAY=192.168.1.10
GATEWAYDEV=eth0
/etc/sysconfig/network-scripts/ifcfg-eth0 文件内容如下：
DEVICE=eth0
IPADDR=192.168.1.3
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=255.255.255.255
ONBOOT=yes
```

参考答案

【问题 1】

（1）A　（2）CNAME

【问题 2】

存在的主要问题：不能区分服务器的差异，也不能反映服务器的当前运行状态（负载量的大小）；或者，不能根据负载情况实现动态调度。

如果一个服务器发生故障不可访问，会造成混乱，一些人能够访问 WWW 服务，另一些则不可以。

【问题 3】

（3）false（或 0）　（4）test.com　（5）192.168.1.10

（6）192.168.1.3　（7）192.168.1.0　（8）255.255.255.255

【问题 4】

主机 ns 同时作为 NFS（网络文件系统）服务器，Web 服务器（www1 和 www2）作为它的客户，共享数据和服务脚本，保证 Web 服务的数据同步或一致。

NFS 服务器需要向 www1 和 www2 分发数据文件，为避免分发和同步占用了 Web 服务的带宽，左边的交换机组成 192.168.2.0 NFS 专用局域网，保证 Web 的服务质量。

同时这种配置将使 NFS 文件系统对外界不可用，增强了服务器的安全性。

试题三（15 分）

阅读以下说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。

【说明】

某公司要在 Windows 2003 Server 上搭建内部 FTP 服务器，服务器分配有一个静态的公网 IP 地址 200.115.12.3。

【问题 1】

在控制面板的“添加/删除程序”对话框中选择<u>（1）</u>，然后进入“应用程序服务器”选项，在<u>（2）</u>组件复选框中选择“文件传输协议（FTP）服务”，就可以在 Windows 2003 中安装 FTP 服务。

备选答案：

（1）A．更改或删除程序　　B．添加新程序

　　C．添加/删除 Windows 组件　　D．设定程序访问和默认值

（2）A．ASP.NET　　B．Internet 信息服务（IIS）

C．应用程序服务器控制台　　D．启用网络服务

【问题 2】

安装完 FTP 服务后，系统建立了一个使用默认端口的“默认 FTP 站点”，若要新建另一个使用“用户隔离”模式的 FTP 站点“内部 FTP 站点”，为了使两个 FTP 服务器不产生冲突，在图 3-1 所示的“内部 FTP 站点”属性对话框中的 IP 地址应配置为__（3）__，端口号应配置为__（4）__。

备选答案：

（3）A．127.0.0.1　　B．200.115.12.3

C．200.115.12.4　　D．192.168.0.0

（4）A．20　　B．21

C．80　　D．服务器 1024～65535 中未用端口号

【问题 3】

在图 3-2 中，新建 FTP 站点的默认主目录为__（5）__。

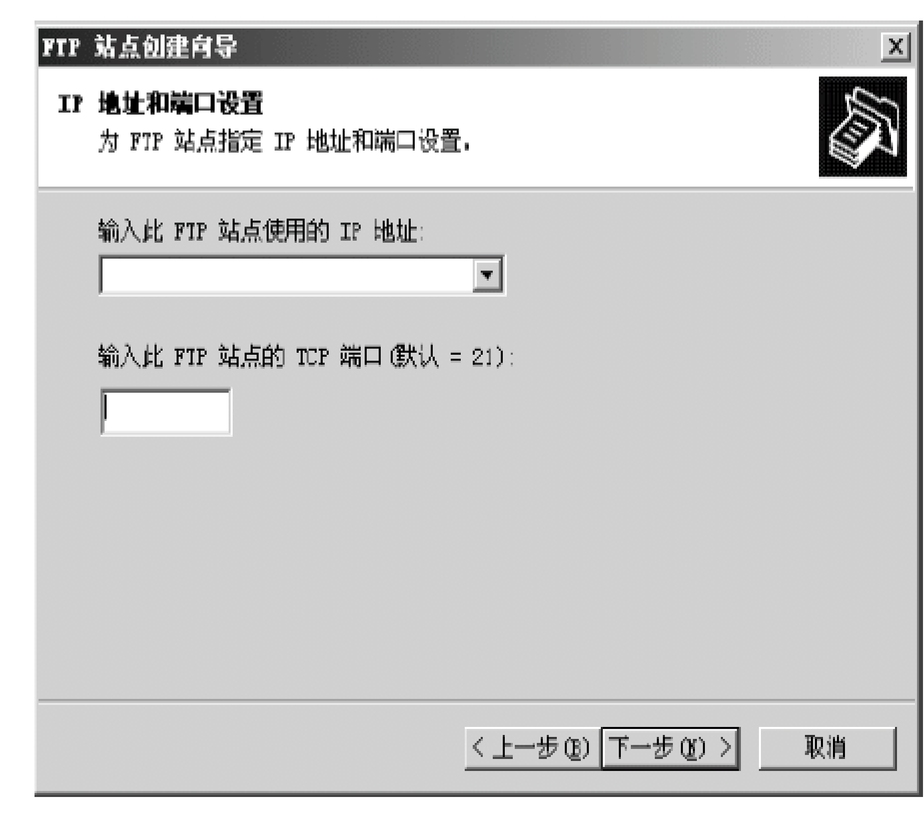


图 3-1

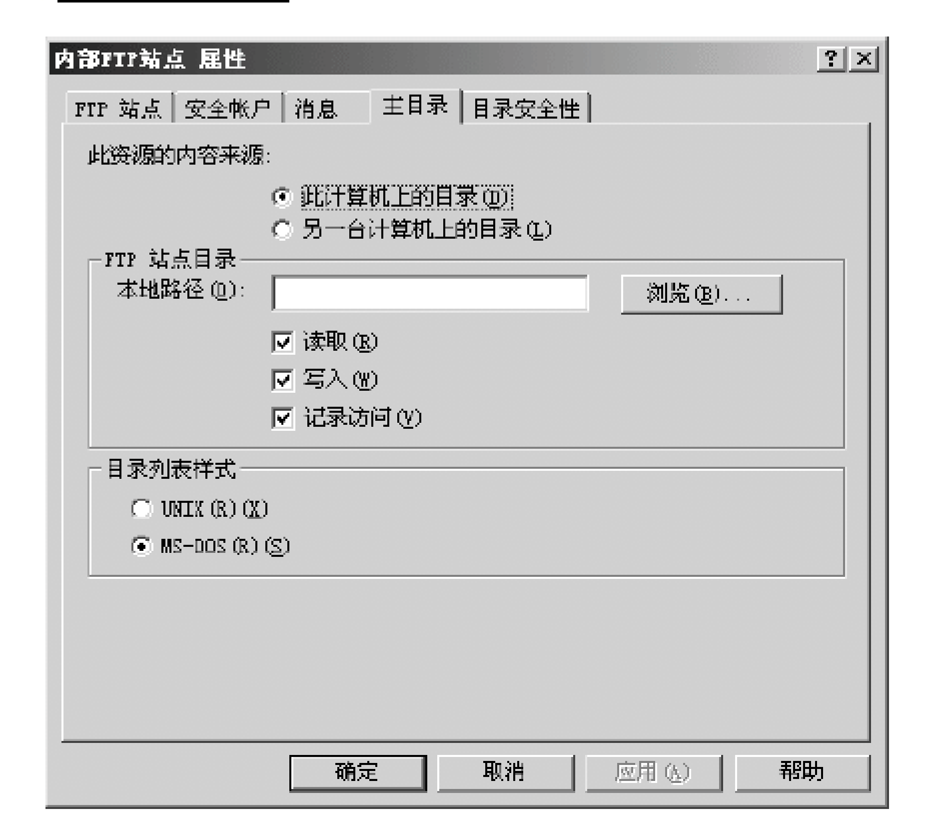


图 3-2

备选答案：

（5）A．C:\inetpub\ftproot　　B．C:\ftp

C．C:\ftp\root　　D．C:\inetpub\wwwroot

【问题 4】

公司要为每个员工在服务器上分配一个不同的 FTP 访问目录，且每个用户只能访问自己目录中的内容，需要进行以下操作：__（6）__和__（7）__。

备选答案：

（6）A．为每个员工分别创建一个 Windows 用户

B．在“内部 FTP 站点”中为每个员工分别创建一个用户

C．为每个员工分别设置一个用户名和密码

（7）A．在主目录下为每个用户创建一个与用户名相同的子目录

B．在主目录下的 Local User 子目录中为每个用户创建一个与用户名相同的子目录

C．在主目录下的 Local User 子目录中为每个用户创建一个子目录，并在 FTP 中设置为用户可访问

D．在主目录下为每个用户创建一个与用户名相同的虚拟目录

【问题 5】

如果还要为其他用户设置匿名登录访问，需要在以上创建用户目录的同一目录下创建名为__（8）__的目录。

备选答案：

（8）A．iUser　　B．users　　C．public　　D．anonymous

【问题 6】

如果公司只允许 IP 地址段 200.115.12.0/25 上的用户访问“内部 FTP 站点”，应进行如下配置。

在图 3-3 所示的对话框中：

（1）选中__（9）__单选按钮；

（2）单击“添加”按钮，打开图 3-4 所示的对话框。

在图 3-4 所示的对话框中：

（1）选中“一台计算机”单选按钮；

（2）在“IP 地址（I）”输入框中填入地址__（10）__，在“子网掩码”输入框中填入 255.255.255.128；

（3）单击“确定”按钮结束配置。

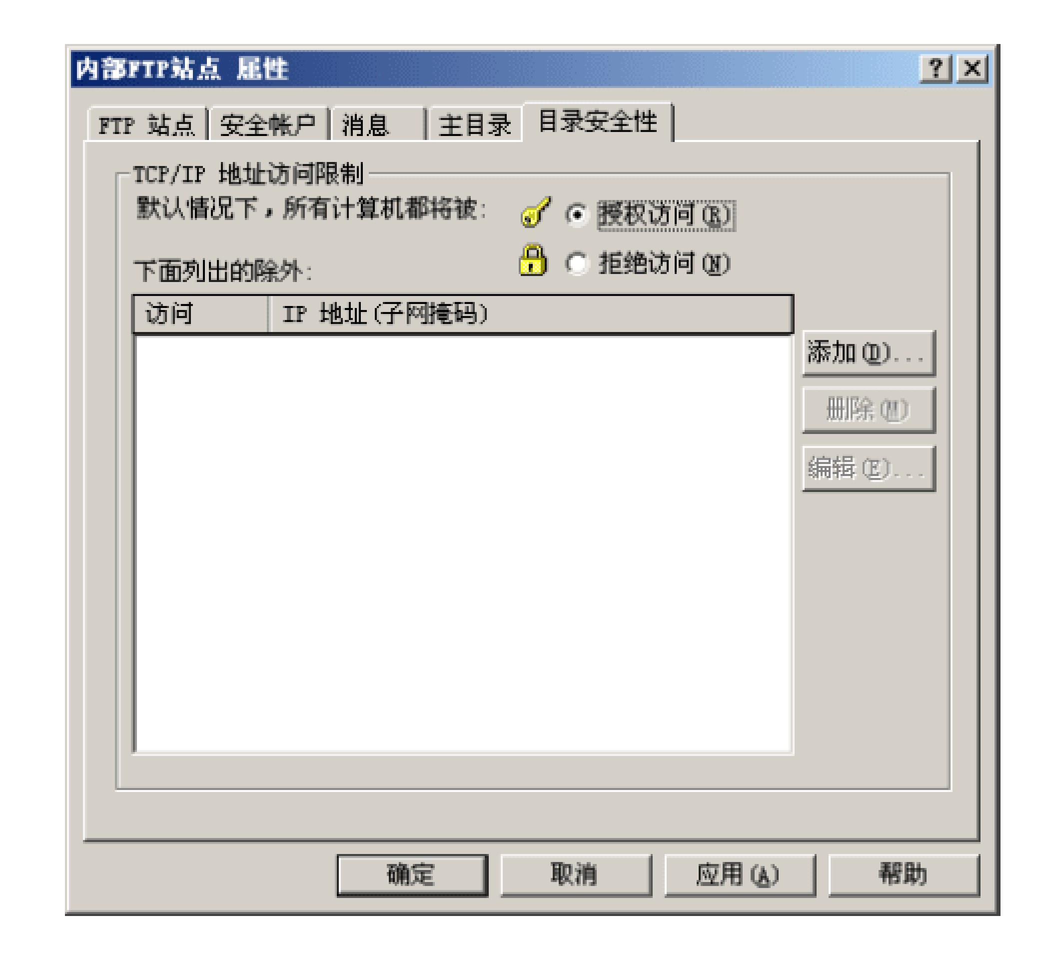


图 3-3



图 3-4

试题三分析

本题考查的是在 Windows 2003 操作系统中安装和配置 FTP 服务的应用，属于 Windows 系统服务配置类的传统题目，考查点也与往年类似。

【问题 1】

考查 FTP 服务的安装过程。

由于架设 FTP 站点需要 IIS6.0 的支持，而在默认状态下 Windows 2003 服务器并没有安装该组件，所以在架设具有用户隔离功能的 FTP 站点之前，需要先安装好 IIS6.0 组件，并将其中的“隔离用户”FTP 组件一并安装成功，下面就是安装“隔离用户”FTP 组件的具体操作步骤。

（1）在 Windows 2003 服务器系统中，依次选择“开始”→“设置”→“控制面板”命令，在弹出的“控制面板”窗口中用鼠标双击其中的“添加或删除程序”图标，在其后出现的“添加或删除程序”设置界面中单击“添加/删除 Windows 组件”按钮，进入到一个标题为“Windows 组件向导”的界面。

（2）在“组件”列表框中，选中“应用程序服务器”复选项，并单击“详细信息”按钮，在随后弹出的“应用程序服务器”设置窗口中，用鼠标双击其中的“Internet 信息服务”项目，进入到“Internet 信息服务”属性设置框，在该设置框的子组件列表中选中“文件传输协议（FTP）服务”项目，单击“确定”按钮。

【问题 2】

考查用户在同一个 IP 地址下配置两个不同 FTP 服务的配置过程。

由于安装 FTP 服务的主机只有一个静态公网 IP 地址 200.115.12.3，因此所有 FTP 服务的 IP 地址均应该配置为该 IP 地址。而 FTP 服务默认配置的端口号为 21，由于此时安装的默认 FTP 服务已经使用了 21 端口号，为了避免冲突，应该使用系统尚未使用的其他端口号。

【问题 3】

考查 FTP 服务安装的默认主目录。在 Windows 操作系统下安装 FTP 服务会默认保存在 C:\ftp\root 目录中。

【问题 4】

考查配置用户隔离模式 FTP 站点的具体操作和配置过程。

为了防止普通用户通过匿名账号访问 FTP 站点，我们在架设 FTP 站点的时候肯定会限制匿名账号的访问权限，只让特定用户才能访问 FTP 站点下面的内容。为此，在正式架设 FTP 站点之前，有必要在 Windows 2003 服务器系统中为 FTP 站点创建一些用户访问账号，此后用户必须凭事先创建好的账号才能登录进行 FTP 站点。在创建 FTP 站点用户访问账号时，可以按照如下步骤进行操作。

（1）在服务器系统桌面中依次选择“开始”→“运行”命令，在弹出的系统运行对话框中，输入字符串命令 compmgmt.msc，按回车键后，打开本地服务器系统的计算机

管理窗口。

（2）在该管理窗口的左侧显示区域中，用鼠标双击“本地用户和组”选项，在其后展开的分支下面选中“用户”文件夹，在对应该文件夹的右侧显示区域中，用鼠标右键单击空白位置，从弹出的右键菜单中选择“新用户”命令，进入“新用户”创建窗口。

（3）在该窗口中设置好用户的访问账号及密码信息，将“用户下次登录时须更改密码”项目的选中状态取消，同时选中“用户不能更该密码”选项与“密码永不过期”选项，再单击“创建”按钮，则一个目标用户的账号信息就算创建成功了。同样地，可以为那些需要访问 FTP 站点的所有用户都创建一个账号信息。

当创建好了用户访问账号后，下面需要进行的操作就是在服务器系统的本地硬盘中创建好 FTP 站点的主目录，以及各个用户账号所对应的用户账号，以便确保每一个用户此后只能访问自己的目录，而没有权利访问其他用户的目录。

为了让架设好的 FTP 站点具有用户隔离功能，必须按照一定的规则设置好该站点的主目录及用户目录。首先需要在 NTFS 格式的磁盘分区中建立一个文件夹，例如该文件夹名称为 aaa，并把该文件夹作为待建 FTP 站点的主目录。

接着进入到 aaa 文件夹窗口中，并在其中创建一个子文件夹，同时必须将该子文件夹名称设置为 LocalUser（该子文件夹名称不能随意设置）。再打开 LocalUser 子文件夹窗口，然后在该窗口下依次创建好与每个用户账号名称相同的个人文件夹。例如可以为 aaa 用户创建一个 aaa 子文件夹（要是用户账号名称与用户目录名称不一样的话，用户就无法访问到自己目录下面的内容）。

做好上面的各项准备工作后，现在就能正式搭建具有“用户隔离”功能的 FTP 站点了，下面就是具体的搭建步骤。

（1）在系统桌面中选择“开始”→“程序”→“管理工具”→“Internet 信息服务（IIS）管理器”命令，打开 IIS 控制台窗口，在该窗口的左侧列表区域，用鼠标右击“FTP 站点”，并从弹出的右键菜单中依次选择“新建”→“FTP 站点”菜单命令，进入到 FTP 站点创建向导设置界面，单击“下一步”按钮。

（2）在弹出的“FTP 站点描述”界面中输入 FTP 站点的名称信息，例如这里可以输入“用户隔离站点”，继续单击“下一步”按钮。在随后出现的 IP 地址和端口设置页面中，设置好目标 FTP 站点的 IP 地址，同时将服务端口号码设置成默认的 21，再单击“下一步”按钮。

接着将看到一个标题为“FTP 用户隔离”的设置界面，选中该界面中的“隔离用户”项目，之后进入到 FTP 站点主目录向导设置窗口，单击其中的“浏览”按钮，从随后弹出的文件夹选择对话框中将前面已经创建好的 aaa 文件夹选中并导入进来，再单击“确定”按钮。当向导窗口要求设置“FTP 站点访问权限”时，必须将“写入”项目选中，最后单击“完成”按钮，结束 FTP 站点的架设操作。

【问题 5】

考查匿名用户访问的主目录。

要是希望架设成功的 FTP 站点具有匿名登录功能的话，那就必须在 LocalUser 文件夹窗口中创建一个 Public 子目录，以后访问者通过匿名方式登录进 FTP 站点时，只能浏览到 Public 子目录中的内容。

【问题 6】

考查控制 IP 地址段用户访问。

如果公司只允许 IP 地址段 200.115.12.0/25 上的用户访问“内部 FTP 站点”，应进行如下配置。

在图 3-3 所示的对话框中：

选中授权访问单选按钮，这样会接受在特定地址范围内的主机访问；

单击“添加”按钮，打开图 3-4 所示的对话框。

在图 3-4 所示的对话框中：

（1）选中“一组计算机”单选按钮；

（2）在“IP 地址”输入框中填入地址 200.115.12.0～200.115.12.127 中的任意一个即可，然后在“子网掩码”输入框中填入 255.255.255.128；

（3）单击“确定”按钮结束配置。

参考答案

【问题 1】

（1）A．添加/删除 Windows 组件（2）B．Internet 信息服务

【问题 2】

（3）B．200.115.12.3　　　　（4）D．服务器 1024～65535 中未用端口号

【问题 3】

（5）A．C:\inetpub\ftproot

【问题 4】

（6）A．为每个员工分别创建一个 Windows 用户

（7）B．在主目录下的 Local User 子目录中为每个用户创建一个与用户名相同的子目录

【问题 5】

（8）C．public

【问题 6】

（9）授权访问

（10）200.115.12.0～200.115.12.127 之一

试题四（15 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

2007 年春，ARP 木马大范围流行。木马发作时，计算机网络连接正常却无法打开网

页。由于 ARP 木马发出大量欺骗数据包，导致网络用户上网不稳定，甚至网络短时瘫痪。

【问题 1】

ARP 木马利用____（1）____协议设计之初没有任何验证功能这一漏洞而实施破坏。

【问题 2】

在以太网中，源主机以____（2）____方式向网络发送含有目的主机 IP 地址的 ARP 请求包；目的主机或另一个代表该主机的系统，以____（3）____方式返回一个含有目的主机 IP 地址及其 MAC 地址对的应答包。源主机将这个地址对缓存起来，以节约不必要的 ARP 通信开销。ARP 协议____（4）____必须在接收到 ARP 请求后才可以发送应答包。

备选答案：

（2）A．单播　　B．多播　　C．广播　　D．任意播

（3）A．单播　　B．多播　　C．广播　　D．任意播

（4）A．规定　　B．没有规定

【问题 3】

ARP 木马利用感染主机向网络发送大量虚假 ARP 报文，主机____（5）____导致网络访问不稳定。例如：向被攻击主机发送的虚假 ARP 报文中，目的 IP 地址为____（6）____，目的 MAC 地址为____（7）____，这样会将同网段内其他主机发往网关的数据引向发送虚假 ARP 报文的机器，并抓包截取用户口令信息。

备选答案：

（5）A．只有感染 ARP 木马时才会　　B．没有感染 ARP 木马时也有可能

C．感染 ARP 木马时一定会　　D．感染 ARP 木马时一定不会

（6）A．网关 IP 地址　　B．感染木马的主机 IP 地址

C．网络广播 IP 地址　　D．被攻击主机 IP 地址

（7）A．网关 MAC 地址　　B．被攻击主机 MAC 地址

C．网络广播 MAC 地址　　D．感染木马的主机 MAC 地址

【问题 4】

网络正常时，运行如下命令，可以查看主机 ARP 缓存中的 IP 地址及其对应的 MAC 地址：

C:\>arp ____（8）____

备选答案：

（8）A．-s　　B．-d　　C．-all　　D．-a

假设在某主机运行上述命令后，显示如图 4-1 中所示信息：

```
Interface: 172.30.1.13 --- 0x30002
  Internet Address      Physical Address      Type
  172.30.0.1            00-10-db-92-aa-30     dynamic
```

图 4-1

00-10-db-92-aa-30 是正确的 MAC 地址。在网络感染 ARP 木马时，运行上述命令可能显示如图 4-2 中所示信息：

```
Interface: 172.30.1.13 --- 0x30002
  Internet Address      Physical Address      Type
  172.30.0.1            00-10-db-92-00-31     dynamic
```

图 4-2

当发现主机 ARP 缓存中的 MAC 地址不正确时，可以执行如下命令清除 ARP 缓存：

C:\>ARP __（9）__

备选答案：

（9）A．-s　　B．-d　　C．-all　　D．-a

之后，重新绑定 MAC 地址。命令如下：

C:\>ARP -s __（10）__ __（11）__

备选答案：

（10）A．172.30.0.1　　B．172.30.1.13

　　C．00-10-db-92-aa-30　　D．00-10-db-92-00-31

（11）A．172.30.0.1　　B．172.30.1.13

　　C．00-10-db-92-aa-30　　D．00-10-db-92-00-31

试题四分析

本题考查的是有关 ARP 协议和 ARP 攻击的基础知识，以及对 ARP 攻击进行简单处理所需要掌握的基础知识。

【问题 1】

考查 ARP 攻击的基本原理。ARP 木马利用 ARP 协议设计之初没有任何验证功能这一漏洞而实施破坏。

【问题 2】

考查 ARP 协议的基础知识。源主机以广播方式向网络发送含有目的主机 IP 地址的 ARP 请求包；目的主机或另一个代表该主机的系统，以单播方式返回一个含有目的主机 IP 地址及其 MAC 地址对的应答包。源主机将这个地址对缓存起来，以节约不必要的 ARP 通信开销。ARP 协议没有规定必须在接收到 ARP 请求后才可以发送应答包，这也是 ARP 协议的重要漏洞之一。

【问题 3】

考查 ARP 攻击的基础知识。感染 ARP 木马的主机会向网络发送大量虚假 ARP 报文，会影响其他主机正常上网。因此，如果某个主机没有感染 ARP 木马，也有可能受其他感染木马的主机发送的虚假报文的影响而导致网络访问不稳定。试题中的例子是一个典型

的 ARP 木马攻击方式，感染 ARP 木马的主机向被攻击主机发送的虚假 ARP 报文中，目的 IP 地址为网关 IP 地址，目的 MAC 地址为感染木马的主机 MAC 地址，将同网段内其他主机发往网关的数据引向发送虚假 ARP 报文的机器。

【问题 4】

考查使用命令行工具 arp 配置 Windows，解决 ARP 攻击的技能。

参考答案

【问题 1】

（1）ARP（或）地址解析协议

【问题 2】

（2）C．广播　　（3）A．单播　　（4）B．没有规定

【问题 3】

（5）B．没有感染 ARP 木马时也有可能

（6）A．网关 IP 地址

（7）D．感染木马的主机 MAC 地址

【问题 4】

（8）D．–a　　（9）B．–d　　（10）A．172.30.0.1

（11）C．00-10-db-92-aa-30

试题五（15 分）

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

如图 5-1 所示，某单位通过 2M 的 DDN 专线接入广域网，该单位内网共分为三个子网。服务器放置在子网 192.168.5.0/24 中，财务部工作站放置在子网 192.168.10.0/24，销售部工作站放置在子网 192.168.50.0/24。该单位申请的公网 IP 地址为 61.246.100.96/29。

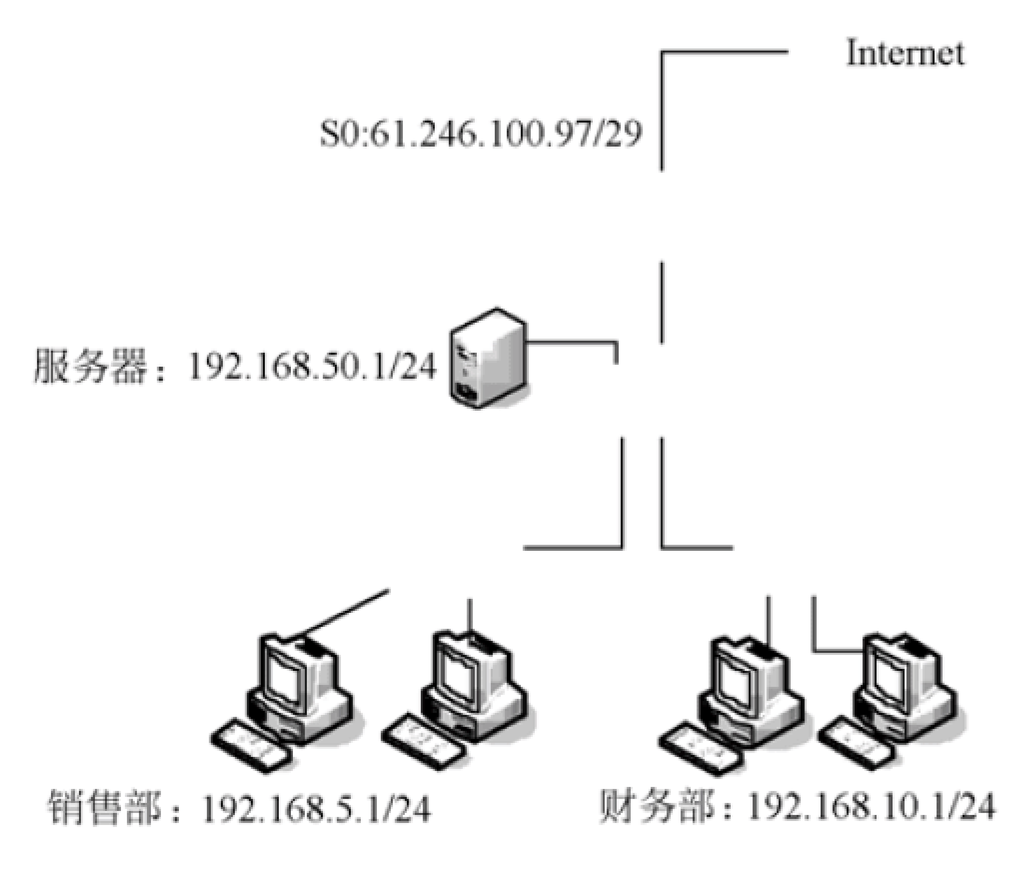


图 5-1

【问题 1】

该单位的公网 IP 地址范围是＿(1)＿到＿(2)＿；其中该单位能够使用的有效公网地址有＿(3)＿个。

【问题 2】

为保证路由器的安全，网络管理员做了如下设置，请阅读下列三段路由配置信息，并在（4）～（6）处填写该段语句的作用。

```
1. Router(Config)#no ip http server                          (4)
2. Router(Config)#snmp-server community admin RW             (5)
3. Router(Config)#access-list 1 permit 192.168.5.1
Router(Config)#line con 0
Router(Config-line)#transport input none
Router(Config-line)#login local
Router(Config-line)#exec-timeout 5 0
Router(Config-line)#access-class 1 in                        (6)
```

【问题 3】

请参照图 5-1，在路由器上完成销售部网段 NAT 的部分配置。

……

Router(config)#ip nat pool xiaoshou 61.246.100.99 61.246.100.99 netmask ＿(7)＿

！设置地址池

！

Router(config)#access-list 2 permit ＿(8)＿ ＿(9)＿

！定义访问控制列表

！

Router(config)#ip nat inside source list 2 pool xiaoshou

！使用访问控制列表完成地址映射

试题五分析

本题考查的是 IP 地址和路由器配置的基本知识。

【问题 1】

根据题目提示，该单位申请的公网 IP 地址为 61.246.100.96/29，因此该单位可用的 IP 地址范围是 61.246.100.96～61.246.100.103。在这些地址中，广播地址，两个互连的路由器使用的接口地址不可用，因此可用地址为 5 个。

【问题 2】

1．Router(Config)#no ip http server　　/*路由器禁止 HTTP 服务*/

　Router (Config)#snmp-server community admin RW　　/*配置路由器读写团体字符串为 admin*/

2．Router(Config)#access-list 1 permit 192.168.5.1

Router(Config)#line con 0

Router(Config-line)#transport input none

Router(Config-line)#login local

Router(Config-line)#exec-timeout 5 0

Router(Config-line)#access-class 1 in　　设置 ACL 允许 192.168.5.1 访问 CON 0

【问题 3】

……

Router(config)#ip nat pool xiaoshou 61.246.100.99 61.246.100.99 netmask 255.255.255.248

！设置地址池

！

Router(config)#access-list 2　permit 192.168.50.0 0.0.0.255

！定义访问控制列表

！

Router(config)#ip nat inside source list 2 pool xiaoshou

！使用访问控制列表完成地址映射

参考答案

【问题 1】

（1）61.246.100.96

（2）61.246.100.103

（3）5

【问题 2】

（4）路由器禁止 HTTP 服务

（5）配置路由器读写团体字符串为 admin

（6）设置 ACL 允许 192.168.5.1 访问 CON 0

【问题 3】

（7）255.255.255.248

（8）192.168.50.0

（9）0.0.0.255

第 15 章　2008 上半年网络工程师上午试题分析与解答

试题（1）

内存采用段式存储管理有许多优点，但__（1）__不是其优点。

（1）A．分段是信息逻辑单位，用户不可见　　B．各段程序的修改互不影响

　　C．地址变换速度快、内存碎片少　　D．便于多道程序共享主存的某些段

试题（1）分析

本题考查操作系统内存管理方面的基本概念。操作系统内存管理方案有许多种，其中，分页存储管理系统中的每一页只是存放信息的物理单位，其本身没有完整的意义，因而不便于实现信息的共享，而段却是信息的逻辑单位，各段程序的修改互不影响，无内碎片，有利于信息的共享。

参考答案

（1）C

试题（2）

现有四级指令流水线，分别完成取指、取数、运算、传送结果 4 步操作。若完成上述操作的时间依次为 9ns、10ns、6ns、8ns，则流水线的操作周期应设计为__（2）__ns。

（2）A．6　　B．8　　C．9　　D．10

试题（2）分析

本题考查计算机流水线基本工作原理。

流水线的基本原理是把一个重复的过程分解为若干个子过程，前一个子过程为下一个子过程创造执行条件，每一个过程可以与其他子过程同时进行。流水线各段执行时间最长的那段为整个流水线的瓶颈，一般地，将其执行时间称为流水线的周期。

参考答案

（2）D

试题（3）

内存按字节编址，地址从 90000H 到 CFFFFH，若用存储容量为 16K×8bit 的存储器芯片构成该内存，至少需要__（3）__片。

（3）A．2　　B．4　　C．8　　D．16

试题（3）分析

本题考查计算机中的存储部件组成。

内存按字节编址,地址从 90000H 到 CFFFFH 时，存储单元数为 CFFFFH－90000H＝

3FFFFH，即 2^{18}B。若存储芯片的容量为 16K×8bit，则需 $2^{18}/16K=2^4$ 个芯片组成该内存。

参考答案

（3）D

试题（4）

__（4）__是一种面向数据流的开发方法，其基本思想是软件功能的分解和抽象。

（4）A．结构化开发方法　　　　B．Jackson 系统开发方法

　　C．Booch 方法　　　　　　D．UML（统一建模语言）

试题（4）分析

本题考查软件开发方法基本概念。结构化开发方法是传统的、也是应用较为广泛的一种软件开发方法，它基于数据流进行需求分析和软件设计，用抽象模型的概念，按照软件内部数据传递和转换关系，对问题和功能自顶向下逐层分解。Jackson 系统开发方法是一种典型的面向数据结构的分析和设计方法，以活动为中心，一连串活动的顺序组合成一个完整的工作进程。Booch 方法是一种面向对象的软件开发方法。UML 仅仅是一种建模标准语言，规定了构成软件的各个元素和构件的图示规范。

参考答案

（4）A

试题（5）

采用 UML 进行软件设计时，可用__（5）__关系表示两类事物之间存在的特殊/一般关系，用聚集关系表示事物之间存在的整体/部分关系。

（5）A．依赖　　B．聚集　　C．泛化　　D．实现

试题（5）分析

本题考查对 UML 中关系概念的理解。按照面向对象技术的描述，若两类事物之间存在特殊/一般关系，则用继承机制表示该关系，即 UML 中的泛化关系。

参考答案

（5）C

试题（6）

某项目制定的开发计划中定义了 3 个任务，其中任务 A 首先开始，且需要 3 周完成，任务 B 必须在任务 A 启动 1 周后开始，且需要 2 周完成，任务 C 必须在任务 A 完成后才能开始，且需要 2 周完成。该项目的进度安排可用下面的甘特图__（6）__来描述。

（6）A．　　　　　　　　　　　　B．





试题（6）分析

本题考查甘特图的概念。甘特图可用来标示一个项目中各任务计划进度和当前进度，能动态反映项目进展情况。甘特图中用水平线表示任务的工作阶段，其起点和终点分别对应任务的开始时间和完成时间，长度表示完成任务的周期。在图 A 和图 C 中，任务 A 结束后任务 B 才开始，在图 B 中，任务 B 和任务 A 同时开始，这些都和题目要求的“任务 B 必须在启动任务 A 后 1 周开始”不符。

参考答案

（6）D

试题（7）

下列叙述中错误的是__（7）__。

（7）A．面向对象程序设计语言可支持过程化的程序设计

B．给定算法的时间复杂性与实现该算法所采用的程序设计语言无关

C．与汇编语言相比，采用脚本语言编程可获得更高的运行效率

D．面向对象程序设计语言不支持对一个对象的成员变量进行直接访问

试题（7）分析

本题程序设计基础知识。

关于脚本语言的基本知识如下：

① 脚本语言（JavaScript，VBScript 等）是介于 HTML 和 C、C++、Java、C#等编程语言之间的程序设计语言。HTML 通常用于格式化和链接文本，而编程语言通常用于向机器发出一系列复杂的指令。

② 脚本语言中也使用变量和函数，这一点与编程语言相似。与编程语言之间最大的区别是编程语言的语法和规则更为严格和复杂。

③ 脚本语言一般都有相应的脚本引擎来解释执行，是一种解释性语言，一般需要解释器才能运行。

④ 脚本语言一般以文本形式存在，类似于一种命令。

下面举例说明脚本语言。设有一个可执行程序 open_aa.exe，用于打开扩展名为“.aa”的文件。编写“.aa”文件需要指定一套规则（语法），open_aa.exe 就用这种规则来理解文件编写人的意图并作出回应。因此，这一套规则就是脚本语言。

汇编语言是符号化的机器语言，一般情况下，用汇编语言编写的程序比高级语言效

率更高。根据脚本语言的以上特点，“采用脚本语言编程可获得更高的运行效率”是错误的。

参考答案

（7）C

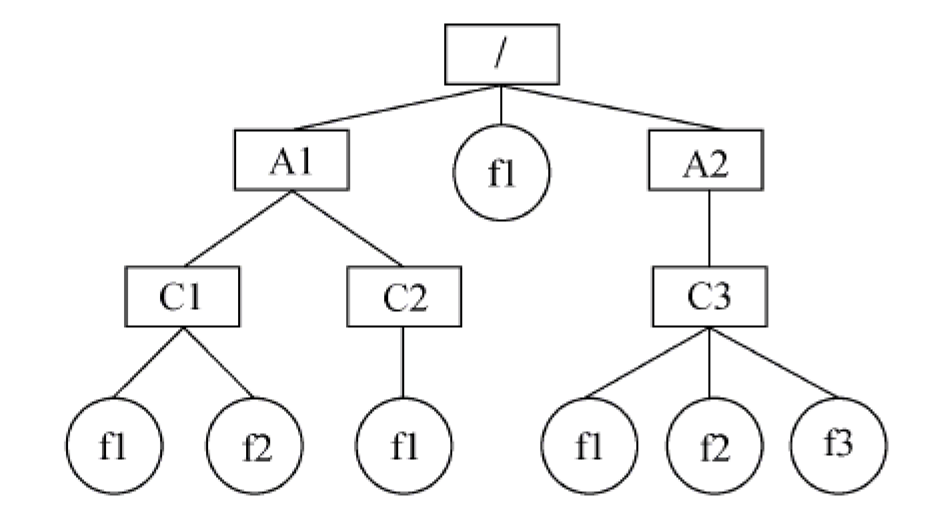
试题（8）、（9）

在下图所示的树型文件系统中，方框表示目录，圆圈表示文件，“/”表示路径中的分隔符，“/”在路径之首时表示根目录。图中，__（8）__。假设当前目录是 A2，若进程 A 以如下两种方式打开文件 f2：

方式①　fd1=open("__（9）__/f2",o_RDONLY);

方式②　fd1=open("/A2/C3/f2",o_RDONLY);

那么，采用方式①的工作效率比方式②的工作效率高。



（8）A．根目录中文件 f1 与子目录 C1、C2 和 C3 中文件 f1 相同

B．子目录 C1 中文件 f2 与子目录 C3 中文件 f2 是相同的

C．子目录 C1 中文件 f2 与子目录 C3 中文件 f2 是不同的

D．子目录 C1 中文件 f2 与子目录 C3 中文件 f2 可能相同也可能不相同

（9）A．/A2/C3　　B．A2/C3　　C．C3　　D．f2

试题（8）、（9）分析

本题考查操作系统中文件系统的树型目录结构的知识。在树型目录结构中，树的根结点为根目录，数据文件作为树叶，其他所有目录均作为树的结点。在树型目录结构中，从根目录到任何数据文件之间，只有一条唯一的通路，从树根开始，把全部目录文件名与数据文件名，依次用“/”连接起来，构成该数据文件的路径名，且每个数据文件的路径名是唯一的。这样，可以解决文件重名问题。所以，对于第（8）题，虽然数据文件名均为 f2，但不一定是相同的文件。正确答案为 D。

从根目录开始的路径名为绝对路径名，如果文件系统有很多级时，使用不是很方便，所以引入相对路径名。引入相对路径名后，当访问当前目录下的文件时，可采用相对路径名，系统从当前目录开始查找要访问的文件，因此比采用绝对路径名，可以减少访问目录文件的次数，提高了系统的工作效率。所以，对于第（9）题，正确答案为 C。

参考答案

（8）D　（9）C

试题（10）

依据我国著作权法的规定，__（10）__属于著作人身权。

（10）A．发行权　　B．复制权
　　C．署名权　　D．信息网络传播权

试题（10）分析

著作权法规定："著作权人可以全部或者部分转让本条第一款第（五）项至第（十七）项规定的权利，并依照约定或者本法有关规定获得报酬。"其中，包括署名权。

参考答案

（10）C

试题（11）、（12）

E1 载波把 32 个信道按__（11）__方式复用在一条 2.048Mb/s 的高速信道上，每条话音信道的数据速率是__（12）__。

（11）A．时分多路　　B．空分多路　　C．波分多路　　D．频分多路
（12）A．56Kb/s　　B．64Kb/s　　C．128Kb/s　　D．512Kb/s

试题（11）、（12）分析

E1 载波是一种时分多路复用信道。在 E1 信道中，8 比特组成一个时槽，32 个时槽编号为 TS0～TS31，组成一个帧。16 个帧组成一个复帧。

在 E1 帧中，TS0 用于传送帧同步信号、循环冗余校验（CRC-4）和端到端的告警指示；TS16 传送随路信令、复帧同步信号和复帧的端到端告警指示；TS1～TS15 和 TS17～TS31 共 30 个时槽传送话音或数据信息。TS1～TS15 和 TS17～TS31 称为净荷，TS0 和 TS16 叫做开销。如果采用带外公共信道信令，则 TS16 也可用来传送信息，这时开销只有 TS0 了。

根据各个时槽的不同用途，可以把 E1 信道的 PCM 编码分为以下几种：

- PCM30：可用时槽为 30 个（TS1～TS15 和 TS17～TS31），TS16 传送信令，无 CRC 校验。
- PCM31：可用时槽为 31 个（TS1～～TS31），采用带外公共信道信令，无 CRC 校验。
- PCM30C：可用时槽为 30 个（TS1～TS15 和 TS17～TS31），TS16 传送信令，有 CRC 校验。
- PCM31C：可用时槽为 31 个（TS1～TS31），采用带外公共信道信令，有 CRC 校验。

E1 线路有以下 3 种使用方式：

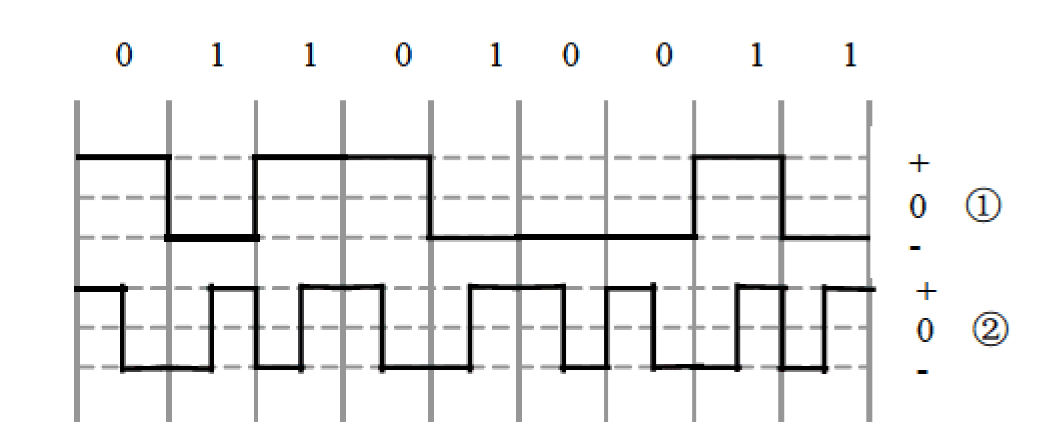
- 将整个 2.048Mb/s 用作一条链路，例如 2Mb/s 的 DDN；
- 将整个带宽用作若干个 64Kb/s 的组合，如 128Kb/s、256Kb/s 等，这就是 CE1。与 E1 一样，CE1 的总带宽也是 2.048Mb/s，但 E1 不能划分子信道，CE1 能划分子信道。CE1 的 TS0 用于传送同步号，TS16 传送控制信令，传送用户数据的只有 30 个时槽；
- 用作电话交换机之间的数字中继，这是 E1 最基本的用法。它把一条 E1 作为 32 个 64Kb/s 的子话音信道来使用，但是 TS0 和 TS16 用作信令控制，所以一条 E1 可以传 30 路话音。ISDN 的 PRI 接口就是这种接入方式。

参考答案

（11）A　（12）B

试题（13）

下图的两种编码方案分别是__（13）__。



（13）A．①差分曼彻斯特编码，②双相码

B．①NRZ 编码，②差分曼彻斯特编码

C．①NRZ-I 编码，②曼彻斯特编码

D．①极性码，②双极性码

试题（13）分析

在图①中，每个“0”比特的前沿没有电平跳变，每个“1”比特的前沿有电平跳变，这是典型的 NRZ-I 编码的波形。NRZ-I 编码的数据速率与码元速率一致，其缺点是当遇到长串的“0”时会失去同步，所以有时要做出某种变通，例如采用 4B/5B 编码。

曼彻斯特编码和差分曼彻斯特编码都属于双相码。双相码要求每一比特中间都有一个电平跳变，它起到自定时的作用。在图②中，我们用高电平到低电平的转换边表示“0”，用低电平到高电平的转换边表示“1”，这是曼彻斯特编码的一种实现方案。反之，如果用高电平到低电平的转换边表示“1”，而用低电平到高电平的转换边表示“0”，也可以认为是曼彻斯特编码，只要能区分两种不同的状态就可以了。比特中间的电平转换边既表示了数据代码，也作为定时信号使用。曼彻斯特编码用在低速以太网中。

差分曼彻斯特编码与曼彻斯特编码不同，码元中间的电平转换边只作为定时信号，而不表示数据。数据的表示在于每一位开始处是否有电平转换：有电平转换表示“0”，

无电平转换表示“1”，差分曼彻斯特编码用在令牌环网中。

在曼彻斯特编码和差分曼彻斯特编码的图形中可以看出，这两种双相码的每一个码元都要调制为两个不同的电平，因而调制速率是码元速率的二倍。这对信道的带宽提出了更高的要求，所以在数据速率很高时实现起来更昂贵，但由于其良好的抗噪声特性和比特同步能力，所以在局域网中仍被广泛使用。

参考答案

（13）C

试题（14）、（15）

假设模拟信号的最高频率为 5MHz，采样频率必须大于__（14）__，才能使得到的样本信号不失真，如果每个样本量化为 256 个等级，则传输的数据速率是__（15）__。

（14）A．5MHz　B．10MHz　C．15MHz　D．20MHz

（15）A．10Mb/s　B．50Mb/s　C．80Mb/s　D．100Mb/s

试题（14）、（15）分析

按照尼奎斯特采样定理，为了恢复原来的模拟信号，取样速率必须大于模拟信号最高频率的二倍，即

$$f=\frac{1}{T}>2f_{max}$$

其中 f 为采样频率，T 为采样周期，f_{max} 为模拟信号的最高频率。所以当模拟信号的频率为 5MHz 时，采样频率必须大于 10MHz。

当样本量空间被量化为 256 个等级时，每个样本必须用 8 比特来表示。根据计算：

$$8\times10\text{MHz}=80\text{Mb/s}$$

参考答案

（14）B　（15）C

试题（16）、（17）

在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 2 位终止位，若每秒钟传送 100 个字符，采用 4 相相位调制，则码元速率为__（16）__，有效数据速率为__（17）__。

（16）A．50 波特　B．500 波特　C．550 波特　D．1100 波特

（17）A．500b/s　B．700b/s　C．770b/s　D．1100b/s

试题（16）、（17）分析

根据题中给出的条件，每个字符要占用 1＋7＋1＋2＝11（位）。每秒钟传送 100 个字符，则数据速率为 11×100＝1100b/s。在采用 4 相相位调制的情况下，数据速率为码元速率的 2 倍，所以码元速率为 550 波特。有效数据速率可计算如下：

$$1100\text{b/s}\times\frac{7}{11}=700\,\text{b/s}$$

参考答案

（16）C　（17）B

试题（18）

设信道带宽为 3400Hz，调制为 4 种不同的码元，根据 Nyquist 定理，理想信道的数据速率为＿（18）＿。

（18）A．3.4Kb/s　　B．6.8Kb/s　　C．13.6Kb/s　　D．34Kb/s

试题（18）分析

按照 Nyquist 定理，

$$B=2W\text{（Baud）}$$

码元速率为信道带宽的两倍。同时数据速率还取决于码元的离散状态数，码元携带的信息量 n（比特数）与码元的离散状态数 N 有如下关系：

$$n=\log_2 N$$

所以，综合考虑了信道带宽和码元的离散状态数后得到的公式为：

$$R=B\log_2 N=2W\log_2 N\text{（b / s）}$$

其中，R 表示数据速率，单位是 b/s。据此，数据速率可计算如下：

$$R=B\log_2 N=2W\log_2 N=2\times 3400\times \log_2 4=6800\times 2=13.6\text{Kb/s}$$

参考答案

（18）C

试题（19）

采用 CRC 校验的生成多项式为 $G(x)=x^{16}+x^{15}+x^2+1$，它产生的校验码是＿（19）＿位。

（19）A．2　　B．4　　C．16　　D．32

试题（19）分析

循环冗余校验码 CRC（Cyclic Redundancy Check）的长度取决于生成多项式的幂次。如果生成多项式为 $G(x)=x^{16}+x^{15}+x^2+1$，则产生的 CRC 校验码必定是 16 位。

参考答案

（19）C

试题（20）

IPv6 地址以 16 进制数表示，每 4 个 16 进制数为一组，组之间用冒号分隔，下面的 IPv6 地址 ADBF:0000:FEEA:0000:0000:00EA:00AC:DEED 的简化写法是＿（20）＿。

（20）A．ADBF:0:FEEA:00:EA:AC:DEED　　B．ADBF:0:FEEA::EA:AC:DEED

C．ADBF:0:FEEA:EA:AC:DEED　　D．ADBF::FEEA::EA:AC:DEED

试题（20）分析

IPv6 地址扩展到 128 位。2^{128} 足够大，这个地址空间可能永远用不完。事实上，这个数大于阿伏加德罗常数，足够为地球上每个分子分配一个 IP 地址。用一个形象的说法，这么大的地址空间允许整个地球表面上每平方米配置 7×10^{23} 个 IP 地址！

IPv6 地址采用冒号分隔的十六进制数表示，例如下面是一个 IPv6 地址：

8000:0000:0000:0000:0123:4567:89AB:CDEF

为了便于书写，规定了一些简化写法。首先，每个字段开始的 0 可以省去，例如 0123 可以简写为 123；其次一个或多个 0000 可以用一对冒号代替。这样，以上地址可简写为：

8000: :123:4567:89AB:CDEF

还有，IPv4 地址仍然保留十进制表示法，只需在前面加上一对冒号，就成为 IPv6 格式，例如：

: :192.168.10.1

参考以上示例，答案 B 是正确的。

参考答案

（20）B

试题（21）

浏览器与 Web 服务器通过建立＿（21）＿连接来传送网页。

（21）A．UDP　　B．TCP　　C．IP　　D．RIP

试题（21）分析

浏览器与 Web 服务器之间通过 HTTP 协议传送网页数据。支持 HTTP 协议的下层协议为 TCP 协议，所以在开始传送网页之前浏览器与 Web 服务器必须先建立一条 TCP 连接。

参考答案

（21）B

试题（22）

在 TCP 协议中，采用＿（22）＿来区分不同的应用进程。

（22）A．端口号　　B．IP 地址　　C．协议类型　　D．MAC 地址

试题（22）分析

TCP 属于传输层协议，它可以支持多种应用层协议。应用层协议访问 TCP 服务的访问点是端口号，不同的端口号用于区分不同的应用进程。例如 HTTP 协议对应的端口号是 80，FTP 对应的端口号是 20 和 21。

参考答案

（22）A

试题（23）、（24）

TCP 是互联网中的传输层协议，使用＿（23）＿次握手协议建立连接。这种建立连接的方法可以防止＿（24）＿。

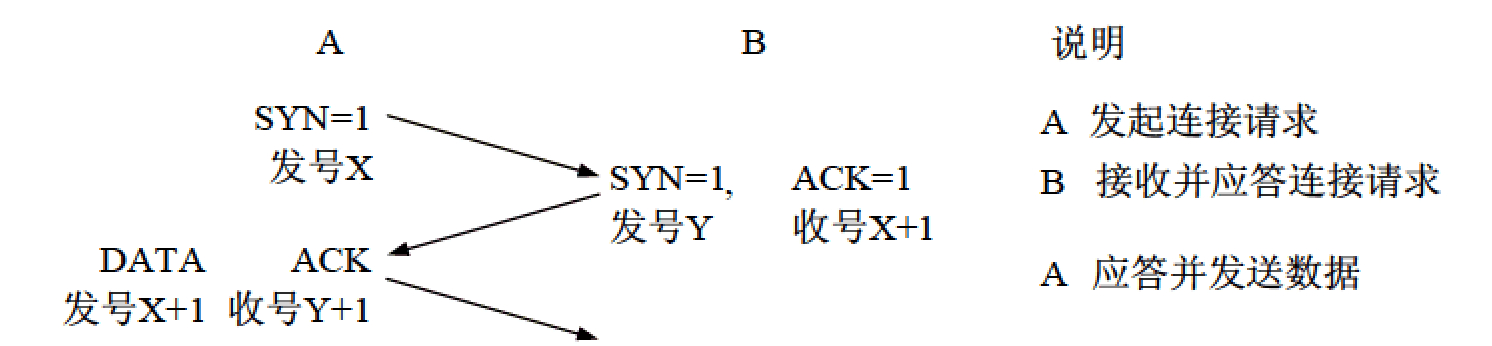
（23）A．1　　B．2　　C．3　　D．4

（24）A．出现半连接　　B．无法连接

C．产生错误的连接　　　　D．连接失效

试题（23）、（24）分析

TCP 协议提供面向连接的服务，采用三次握手建立连接。首先是发起方发送一个 SYN 置位的段，其中的发送顺序号为某个值 X，称为初始顺序号 ISN（Initial Sequence Number）。接收方以 SYN 和 ACK 置位的段响应，其中的应答顺序号应为 X＋1（表示期望从第 X+1 个字节处开始接收数据），发送顺序号为某个值 Y（接收端指定的 ISN）。这个段到达发起端后，发起端以 ACK 置位、应答顺序号为 Y＋1 的段回答，这时连接就正式建立了。如下图所示：



这种建立连接的方式可以防止产生错误的连接。产生错误连接的主要因素来源于网络失效期间存储在网络中的连接请求，这些过期连接请求在网络故障恢复后可能继续到达目标端，干扰新发出的连接请求，从而建立错误的连接。三次握手协议不能防止由于网络失效而出现半连接的情况，对于这种故障，TCP 协议用超时定时器来排除。考虑到基础的 IP 网络提供的服务是不可靠的，所以 TCP 协议还规定了很多类似的超时定时器，来应付各种连接失效的故障。

参考答案

（23）C　（24）C

试题（25）

ARP 协议的作用是由 IP 地址求 MAC 地址，ARP 请求是广播发送，ARP 响应是<u>（25）</u>发送。

（25）A．单播　　B．组播　　C．广播　　D．点播

试题（25）分析

ARP 协议的作用是由 IP 地址求 MAC 地址，其协议数据单元格式如下图所示：

硬件类型		协议类型
硬件地址长度	协议地址长度	操　作
发送结点硬件地址		
发送结点协议地址		
目标结点硬件地址		
目标结点协议地址		

当源主机要发送一个数据帧时，必须在本地的 ARP 表中查找目标主机的 MAC（硬

件）地址。如果 ARP 表查不到，就广播一个 ARP 请求分组，这种分组可到达同一子网中的所有主机，它的含义是："如果你的 IP（协议）地址是这个，请回答你的 MAC 地址是什么。"收到该分组的主机一方面可以用分组中（发送结点的）的两个源地址更新自己的 ARP 表，另一方面用自己的 IP 地址与目标 IP 地址字段比较，若相符则发回一个 ARP 响应分组，向发送方报告自己的 MAC 地址，若不相符则不予回答。ARP 请求通过广播帧发送，ARP 响应通过单播帧发送给源站。

参考答案

（25）A

试题（26）

下面有关 BGP4 协议的描述中，不正确的是__（26）__。

（26）A．BGP4 是自治系统之间的路由协议

B．BGP4 不支持 CIDR 技术

C．BGP4 把最佳通路加入路由表并通告邻居路由器

D．BGP4 封装在 TCP 段中传送

试题（26）分析

互联网由不同的自治系统互连而成，不同的自治系统可能采用不同的路由表，不同的路由选择算法。在不同自治系统之间用外部网关协议（Exterior Gateway Protocol, EGP）交换路由信息。最新的 EGP 协议叫做 BGP（Border Gateway Protocol）。BGP 的主要功能是控制路由策略，例如是否愿意转发过路的分组等。BGP 的 4 种报文表示在下表中，这些报文通过 TCP 连接传送。BGP 支持 CIDR 技术。

报 文 类 型	功 能 描 述
建立（Open）	建立邻居关系
更新（Update）	发送新的路由信息
保持活动状态（Keepalive）	对 Open 的应答/周期性地确认邻居关系
通告	报告检测到的错误

参考答案

（26）B

试题（27）

ICMP 协议在网络中起到了差错控制和交通控制的作用。如果在 IP 数据报的传送过程中，如果出现网络拥塞，则路由器发出__（27）__报文。

（27）A．路由重定向　　B．目标不可到达

C．源抑制　　D．超时

试题（27）分析

ICMP（Internet control Message Protocol）属于网络层协议，用于传送有关通信问题

的消息。ICMP 报文封装在 IP 数据报中传送，因而不保证可靠的提交。ICMP 报文有很多种类，用于表达不同的路由控制信息，其报文格式如下图所示。其中的类型字段表示 ICMP 报文的类型，代码字段可表示报文的少量参数，当参数较多时写入 32 位的参数字段，ICMP 报文携带的信息包含在可变长的信息字段中，校验和字段是关于整个 ICMP 报文的校验和。

<table>
<tr><td>类　型</td><td>代　码</td><td>校　验　和</td></tr>
<tr><td colspan="3">参　数</td></tr>
<tr><td colspan="3">信息（可变长）</td></tr>
</table>

下面简要解释 ICMP 各类报文的含义。

- 目标不可到达（类型 3）：如果路由器判断出不能把 IP 数据报送达目标主机，则向源主机返回这种报文。另一种情况是目标主机找不到有关的用户协议或上层服务访问点，也会返回这种报文。出现这种情况的原因可能是 IP 头中的字段不正确；或是数据报中说明的源路由无效；也可能是路由器必须把数据报分段，但 IP 头中的 D 标志已置位。
- 超时（类型 11）：路由器发现 IP 数据报的生存期已超时，或者目标主机在一定时间内无法完成重装配，则向源端返回这种报文。
- 源抑制（类型 4）：这种报文提供了一种流量控制的初等方式。如果路由器或目标主机缓冲资源耗尽而必须丢弃数据报，则每丢弃一个数据报就向源主机发回一个源抑制报文，这时源主机必须减小发送速度。另外一种情况是系统的缓冲区已用完，并预感到行将发生拥塞，则发出源抑制报文。但是与前一种情况不同，涉及的数据报尚能提交给目标主机。
- 参数问题（类型 12）：如果路由器或主机判断出 IP 头中的字段或语义出错，则返回这种报文，报文头中包含一个指向出错字段的指针。
- 路由重定向（类型 5）：路由器向直接相连的主机发出这种报文，告诉主机一个更短的路径。例如路由器 R1 收到本地网络上的主机发来的数据报，R1 检查它的路由表，发现要把数据报发往网络 X，必须先转发给路由器 R2，而 R2 又与源主机在同一网络中。于是 R1 向源主机发出路由重定向报文，把 R2 的地址告诉它。
- 回声（请求/响应，类型 8/0）：用于测试两个结点之间的通信线路是否畅通。收到回声请求的结点必须发出回声响应报文。该报文中的标识符和序列号用于匹配请求和响应报文。当连续发出回声请求时，序列号连续递增。常用的 PING 工具就是这样工作的。
- 时间戳（请求/响应，类型 13/14）：用于测试两个结点之间的通信延迟时间。请求方发出本地的发送时间，响应方返回自己的接收时间和发送时间。这种应答

过程如果结合强制路由的数据报实现，则可以测量出指定线路上的通信延迟。

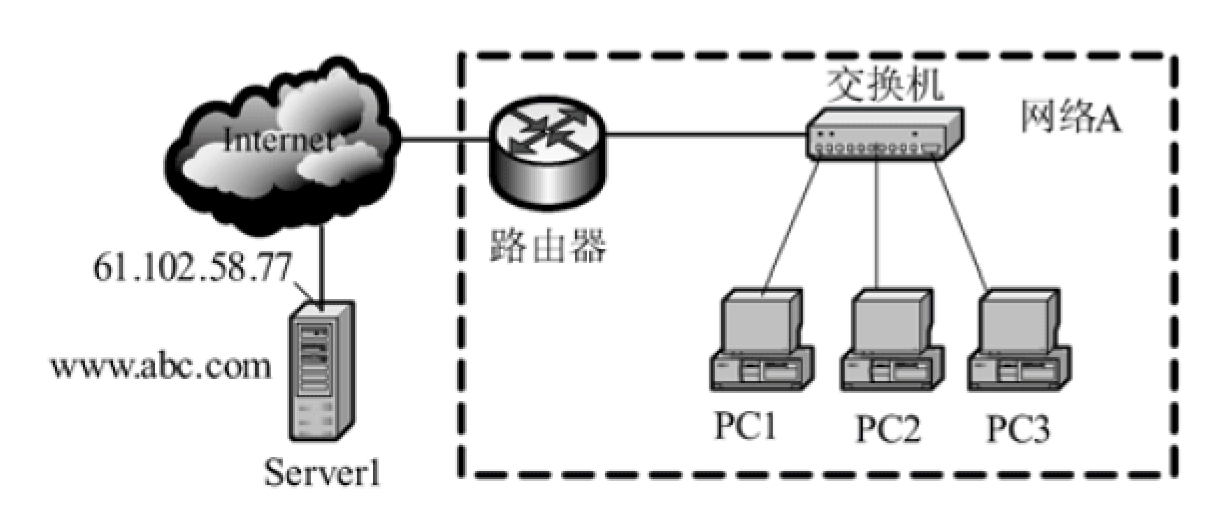
- 地址掩码（请求/响应，类型 17/18）：主机可以利用这种报文获得它所在的 LAN 的子网掩码。首先主机广播地址掩码请求报文，同一 LAN 上的路由器以地址掩码响应报文回答，告诉请求方需要的子网掩码。了解子网掩码可以判断出数据报的目标结点与源结点是否在同一 LAN 中。

参考答案

（27）C

试题（28）～（30）

某网络结构如下图所示。在 Windows 操作系统中，Server1 通过安装__（28）__组件创建 Web 站点。PC1 的用户在浏览器地址栏中输入 www.abc.com 后无法获取响应页面，管理人员在 Windows 操作系统下可以使用__（29）__判断故障发生在网络 A 内还是网络 A 外。如果使用 ping 61.102.58.77 命令对服务器 Server1 进行测试，响应正常，则可能出现的问题是__（30）__。



（28）A. IIS　　B. IE　　C. WWW　　D. DNS

（29）A. ping　61.102.58.77　　B. tracert　61.102.58.77

　　C. netstat　61.102.58.77　　D. arp　61.102.58.77

（30）A. 网关故障　　B. 线路故障

　　C. 域名解析故障　　D. 服务器网卡故障

试题（28）～（30）分析

本题主要考查 Internet 配置及简单故障排除方面知识。

IIS 是建立 Internet /Intranet 的基本组件，通过超文本传输协议（HTTP）传输信息，还可配置 IIS 以提供文件传输协议（FTP）和其他服务。他不同于一般的应用程序，就像驱动程序一样是操作系统的一部分，具有在系统启动时被同时启动的服务功能。Internet Explorer（简称 IE）是由微软公司基于 Mosaic 开发的浏览器。与Netscape类似，IE 内置了一些应用程序，具有浏览、发信、下载软件等多种网络功能。万维网（World Wide Web，WWW）是在因特网上以超文本为基础形成的信息网。万维网为用户提供了一个可以浏览的图形化界面，用户通过它可以查阅 Internet 上的信息资源。互联网常用的服务包括：WWW、Email、FTP、Usenet、IM 等。DNS 是域名系统的缩写，该系统用于命名组织到

域层次结构的映射。故（28）选 A。

ping 用以测试与目的主机的连通性；tracert 命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间；netstat 显示当前所有连接及状态信息；arp 用于通过 IP 地址查询 MAC 地址。故（29）选 B。

如果使用 ping 61.102.58.77 命令对服务器 Server1 进行测试，响应正常，说明与目的主机的连通性正常，故可排除网关故障、线路故障及服务器网卡故障。故（30）选 C。

参考答案

（28）A　（29）B　（30）C

试题（31）、（32）

以下是在 Linux 操作系统中键入 ps 命令后得到的进程状态信息，其中处于“僵死”状态进程的 PID 为<u>（31）</u>，若要终止处于“运行”状态的进程的父进程，可以键入命令<u>（32）</u>。

```
[root@localhost ~]# ps -el | more
F S  UID   PID  PPID  C PRI NI ADDR   SZ WCHAN TTY     TIME     CMD
4 W    0  9822  9521  0  81  0   -  1220 wait4  pts/2  00:00:00  su
4 S    0  9970  9822  0  75  0   -  1294 wait4  pts/2  00:00:00  bash
1 R    0 15354  9970  0  80  0   -   788  -     pts/2  00:00:00  ps
5 Z    0 17658  9976  0  86  0   -   670  -     pts/2  00:00:03  aio/0
```

（31）A．9822　　B．9970　　C．15354　　D．17658

（32）A．kill 9822　　B．kill 9970　　C．python 9521　　D．python 9976

试题（31）、（32）分析

进程就是运行中的程序。一个运行着的程序，可能有多个进程。比如 LinuxSir.Org 所用的 WWW 服务器是 apache 服务器，当管理员启动服务后，可能会有好多人来访问，也就是说许多用户来同时请求 httpd 服务，apache 服务器将会创建有多个 httpd 进程来对其进行服务。

进程一般分为交互进程、批处理进程和守护进程三类。值得一提的是守护进程总是活跃的，一般是后台运行，守护进程一般是由系统在开机时通过脚本自动激活启动或超级管理用户 root 来启动。比如在 Fedora 或 Redhat 中，我们可以定义 httpd 服务器的启动脚本的运行级别，此文件位于/etc/init.d 目录下，文件名是 httpd，/etc/init.d/httpd 就是 httpd 服务器的守护程序，当把它的运行级别设置为 3 和 5 时，当系统启动时，它会跟着启动。

```
[root@localhost ～]# chkconfig  --level 35  httpd on
```

由于守护进程是一直运行着的，所以它所处的状态是等待请求处理任务。比如，我们是不是访问 LinuxSir.Org，LinuxSir.Org 的 httpd 服务器都在运行，等待着用户来访问，也就是等待着任务处理。

Linux 中的进程的有以下常用属性：

- 进程 ID（PID)：是唯一的数值，用来区分进程；
- 父进程和父进程的 ID（PPID)；
- 启动进程的用户 ID（UID）和所归属的组（GID）；
- 进程状态：状态分为运行 R、休眠 S、僵尸 Z；
- 进程执行的优先级；
- 进程所连接的终端名；
- 进程资源占用：比如占用资源大小（内存、CPU 占用量）。

父进程和子进程的关系是管理和被管理的关系，当父进程终止时，子进程也随之而终止。但子进程终止，父进程并不一定终止。比如 httpd 服务器运行时，我们可以杀掉其子进程，父进程并不会因为子进程的终止而终止。在进程管理中，当我们发现占用资源过多，或无法控制的进程时，应该杀死它，以保护系统的稳定安全运行。

进程通常有以下几类状态：

D　Uninterruptible sleep（usually IO）

R　正在运行可中在队列中可过行的；

S　处于休眠状态；

T　停止或被追踪；

W　进入内存交换；

Z　僵死进程；

终止一个进程或终止一个正在运行的程序，一般是通过 kill、killall、pkill、xkill 等进行的。比如一个程序已经死掉，但又不能退出，这时就应该考虑应用这些工具。另外应用的场合就是在服务器管理中，在不涉及数据库服务器程序的父进程的停止运行，也可以用这些工具来终止。为什么数据库服务器的父进程不能用这些工具杀死呢？原因很简单，这些工具在强行终止数据库服务器时，会让数据库产生更多的文件碎片，当碎片达到一定程度的时候，数据库就有崩溃的危险。比如 mysql 服务器最好是按其正常的程序关闭，而不是用 pkill mysqld 或 killall mysqld 这样危险的动作；当然对于占用资源过多的数据库子进程，我们应该用 kill 来杀掉。

参考答案

（31）D　（32）B

试题（33）

若 Linux 用户需要将 FTP 默认的 21 号端口修改为 8800，可以修改<u>（33）</u>配置文件。

（33）A．/etc/vsftpd/userconf　　B．/etc/vsftpd/vsftpd.conf

C．/etc/resolv.conf　　D．/etc/hosts

试题（33）分析

VSFTPD 的配置文件/etc/vsftpd/vsftpd.conf 是个文本文件。以“#”字符开始的行是

注释行。每个选项设置为一行，格式为“option=value”，注意“=”号两边不能留空白符。除了这个主配置文件外，还可以给特定用户设定个人配置文件，具体介绍见后。

:-)VSFTPD 包中所带的 vsftpd.conf 文件配置比较简单，而且非常偏执狂的（文档自称）。我们可以根据实际情况对其进行一些设置，以使得 VSFTPD 更加可用。

- 监听地址与控制端口

listen_address=ip address

此参数在 VSFTPD 使用单独（standalone）模式下有效。此参数定义了在主机的哪个 IP 地址上监听 FTP 请求，即在哪个 IP 地址上提供 FTP 服务。对于只有一个 IP 地址的主机，不需要使用此参数。对于多址主机，不设置此参数，则监听所有 IP 地址。默认值为无。

listen_port=port_value

指定 FTP 服务器监听的端口号（控制端口），默认值为 21。此选项在 standalone 模式下生效。

- FTP 模式与数据端口

FTP 分为两类：PORT FTP 和 PASV FTP。PORT FTP 是一般形式的 FTP。这两种 FTP 在建立控制连接时操作是一样的，都是由客户端首先和 FTP 服务器的控制端口（默认值为 21）建立控制链接，并通过此链接进行传输操作指令。它们的区别在于使用数据传输端口（ftp- data）的方式。PORT FTP 由 FTP 服务器指定数据传输所使用的端口，默认值为 20。PASV FTP 由 FTP 客户端决定数据传输的端口。PASV FTP 这种做法，主要是考虑到存在防火墙的环境下，由客户端与服务器进行沟通（客户端向服务器发出数据传输请求中包含了数据传输端口），决定两者之间的数据传输端口更为方便一些。

port_enable=YES|NO

在数据连接时取消 PORT 模式，设此选项为 NO。它的默认值为 YES。

connetc_from_port_20=YES|NO

控制以 PORT 模式进行数据传输时是否使用 20 端口（ftp-data）。YES 使用，NO 不使用。默认值为 NO，但 RHL 自带的 vsftpd.conf 文件中此参数设为 YES。

参考答案

（33）B

试题（34）

在 Windows Server 2003 的“管理您的服务器”界面中，可以通过<u>（34）</u>安装配置 DHCP 服务器。

（34）A．Active Directory　　B．管理服务器角色
　　　C．IIS 6.0　　D．代理服务器

试题（34）分析

可以通过管理服务器角色来安装配置 DHCP 服务器。

参考答案

（34）B

试题（35）、（36）

在 Windows 环境下，DHCP 客户端可以使用（35）命令重新获得 IP 地址，这时客户机向 DHCP 服务器发送一个（36）数据包来请求租用 IP 地址。

（35）A．ipconfig/release　　B．ipconfig/reload
　　　C．ipconfig/renew　　D．ipconfig/all

（36）A．Dhcpoffer　　B．Dhcpack
　　　C．Dhcpdiscover　　D．Dhcprequest

试题（35）、（36）分析

本题考查的 Windows 环境下 DHCP 的命令。

在 DHCP 客户端上，在 DOS 提示符下输入“ipconfig/all”命令，即可查看客户端 TCP/IP 的详细配置信息。此时可以在客户端运行“ipconfig/release”命令，手工释放 IP 地址。运行“ipconfig/renew”命令可以重新向 DHCP 服务器申请 IP 地址，此时，客户机向 DHCP 服务器发送一个 Dhcpdiscover 数据包来请求租用 IP 地址。

参考答案

（35）C　（36）C

试题（37）、（38）

下图是在 Windows 客户端 DOS 窗口中使用 nslookup 命令后的结果，该客户端的首选 DNS 服务器的 IP 地址是（37）。在 DNS 服务器中，ftp.test.com 是采用新建（38）方式建立的。



（37）A．192.168.21.252　　B．10.10.20.3
　　　C．10.10.20.1　　D．以上都不是

（38）A．邮件交换器　　B．别名
　　C．域　　D．主机

试题（37）、（38）分析

本题考查的是 DNS 服务器的配置和查询。

在 Windows 客户端 DOS 窗口中使用 nslookup 命令可以查看本机的 DNS 服务器配置。其中：

Server: ns1.test.com 表示 dns 服务器名称为 ns1.test.com。

Address: 192.168.21.252 表示 dns 服务器 IP 地址为 192.168.21.252。

Aliases:ftp.test.com 表示 ftp.test.com 是按照别名创建的。

参考答案

（37）A　（38）B

试题（39）

用户可以通过 http://www.a.com 和 http://www.b.com 访问在同一台服务器上（39）不同的两个 Web 站点。

（39）A．IP 地址　　B．端口号
　　C．协议　　D．虚拟目录

试题（39）分析

本题考查的是 IIS 下多站点的配置。

在 IIS 下配置多站点时，可以采用虚拟主机和虚拟目录两种方式。

采用虚拟目录时，发布的站点没有独立域名，而是在主域名下建立虚拟目录，从题目要求看，需要两个独立的域名，所以不可实现。

采用虚拟主机时有三种方式，使用不同 IP 地址，不同端口号和不同的主机头。

使用不同 IP 地址时要求 WEB 服务器配备多网卡，使用不同端口号时，要求在访问 Web 服务器虚拟主机时指名端口号，例如：http://www.b.com:8080，使用不同主机头时，在 IIS 发布中要做主机头域名指定。

从题目选项中可见，只有 A 选项符合要求。

参考答案

（39）A

试题（40）

在 Windows 操作系统下，FTP 客户端可以使用（40）命令显示客户端当前目录中的文件。

（40）A．dir　　B．list　　C．!dir　　D．!list

试题（40）分析

本题考查的是 FTP 命令。常用的 FTP 客户端命令如下：

1．“dir”命令，用来显示 FTP 服务器端有哪些文件可供下载。如果是 FTP 服务器

端，选取 UNIX 的列表风格显示 FTP 服务器端的文件信息，可使用“ftp>ls –l”命令显示。

2．“get”命令，用来从服务器端下载一个文件。

3．“!dir”命令，用来显示客户端当前目录中的文件信息。

4．“put”命令，用来向 FTP 服务器端上传一个文件。

5．“lcd”命令，用来设置客户端当前的目录。

6．“bye”命令，用来退出 FTP 连接。

参考答案

（40）C

试题（41）、（42）

如果希望别的计算机不能通过 ping 命令测试服务器的连通情况，可以__（41）__。如果希望通过默认的 Telnet 端口连接服务器，则下面对防火墙配置正确的是__（42）__。

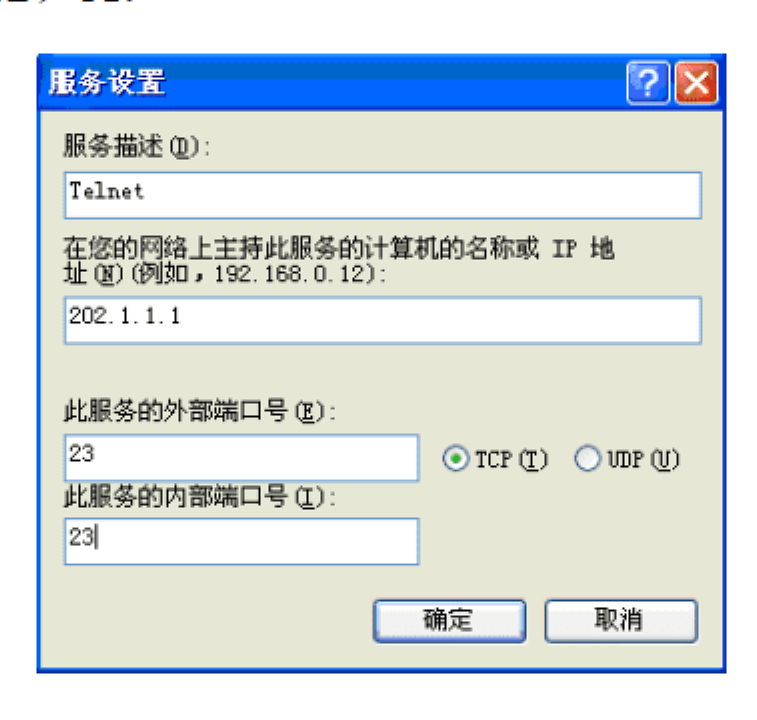
（41）A．删除服务器中的 ping.exe 文件

B．删除服务器中的 cmd.exe 文件

C．关闭服务器中 ICMP 端口

D．关闭服务器中的 Net Logon 服务

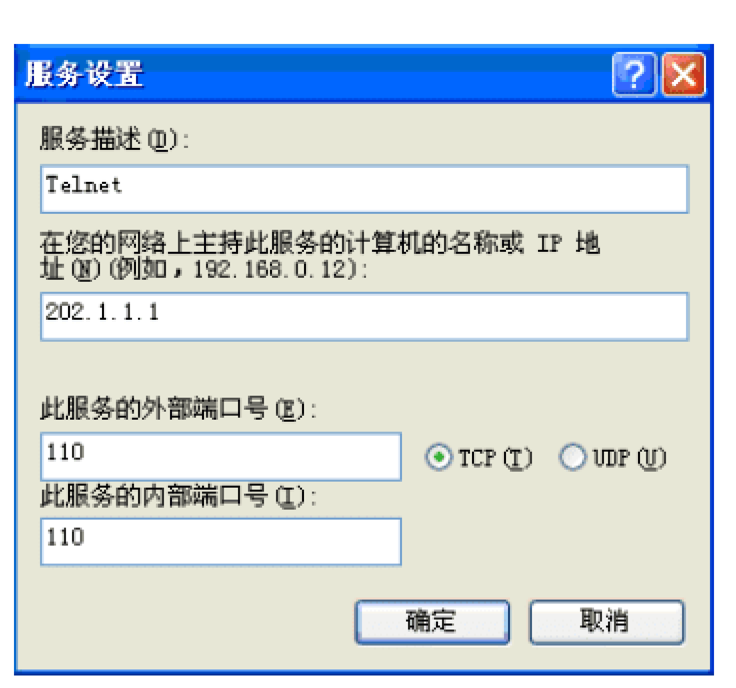
（42）A.



B.

服务设置
服务描述(D):
Telnet
在您的网络上主持此服务的计算机的名称或 IP 地址(N)(例如，192.168.0.12):
202.1.1.1
此服务的外部端口号(E):
23
TCP(T)
UDP(U)
此服务的内部端口号(I):
23
确定
取消

C.



D.

服务设置
服务描述(D):
Telnet
在您的网络上主持此服务的计算机的名称或 IP 地址(N)(例如，192.168.0.12):
202.1.1.1
此服务的外部端口号(E):
110
TCP(T)
UDP(U)
此服务的内部端口号(I):
110
确定
取消

试题（41）、（42）分析

删除服务器中的 ping.exe 和 cmd.exe 会影响服务器运行 ping 命令和一些基于命令行的程序。ping 命令测试机器联通情况实际上是使用了 ICMP 协议，因此，关闭服务器中的 ICMP 端口可以使别的计算机不能通过 ping 命令测试服务器的连通情况。

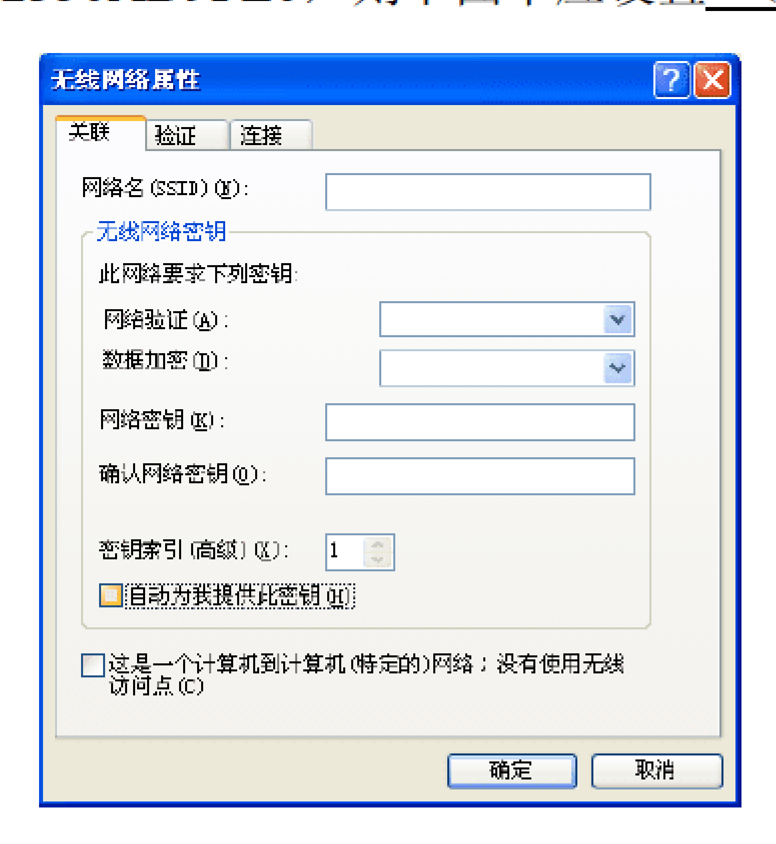
Telnet 使用的是 TCP 协议，缺省情况下使用 23 端口。因此，选题（42）答案为 A。

参考答案

（41）C　（42）A

试题（43）

设置计算机的无线网卡，使该计算机与实验室的无线访问点 LabAP 之间的通信能够受密码保护，指定密钥为 2350AD9FE0，则下图中应设置__（43）__。



（43）A．SSID 为 LabAP，网络验证为开放式，数据加密为 WEP

B．SSID 为 2350AD9FE0，网络验证为开放式，数据加密为 WEP

C．SSID 为 LabAP，网络验证为 WEP，数据加密为开放式

D．SSID 为 2350AD9FE0，网络验证为 WEP，数据加密为开放式

试题（43）分析

题干中的 LabAP 实际上就是 SSID，网络验证为开放式，数据加密为 WEP。因此选择答案 A。

参考答案

（43）A

试题（44）

下面的选项中，属于传输层安全协议的是__（44）__。

（44）A．IPSec　　B．L2TP　　C．TLS　　D．PPTP

试题（44）分析

IPSec 是网络层安全协议，L2TP 和 PPTP 是链路层安全协议，TLS 是传输层安全

协议。

参考答案

（44）C

试题（45）

某银行为用户提供网上服务，允许用户通过浏览器管理自己的银行账户信息。为保障通信的安全，该 Web 服务器可选的协议是__（45）__。

（45）A．POP　　B．SNMP　　C．HTTP　　D．HTTPS

试题（45）分析

POP 是邮局协议，用于接收邮件；SNMP 是简单网络管理协议，用于网络管理；HTTP 是超文本传输协议，众多 Web 服务器都使用 HTTP，但是它不是安全的协议；HTTPS 是安全的超文本传输协议。

参考答案

（45）D

试题（46）

__（46）__不属于电子邮件协议。

（46）A．POP3　　B．SMTP　　C．IMAP　　D．MPLS

试题（46）分析

本题考查的是于电子邮件协议。

POP3（Post Office Protocol 3）协议是适用于 C/S 结构的脱机模型的电子邮件协议。SMTP（Simple Mail Transfer Protocol）协议是简单邮件传输协议。IMAP（Internet Message Access Protocol）是由美国华盛顿大学所研发的一种邮件获取协议。MPLS（Multiprotocol Label Switch）即多协议标记交换，是一种标记（label）机制的包交换技术。

参考答案

（46）D

试题（47）

某客户端采用 ping 命令检测网络连接故障时，发现可以 ping 通 127.0.0.1 及本机的 IP 地址，但无法 ping 通同一网段内其他工作正常的计算机的 IP 地址。该客户端的故障可能是__（47）__。

（47）A．TCP/IP 协议不能正常工作　　B．本机网卡不能正常工作
　　C．本机网络接口故障　　D．本机 DNS 服务器地址设置错误

试题（47）分析

本题考查的是 ping 命令的使用。

采用 ping 命令检测网络连接故障时，可以先输入 ping 127.0.0.1，该地址是本地循环地址，如发现本地址无法 ping 通，就表明本地机 TCP/IP 协议不能正常工作。

如果上面的操作成功，可 ping 通的话，我们接下来可以 Ping 本机 IP，通则表明网

络适配器（网卡或 MODEM）工作正常，不通则是网络适配器出现故障。

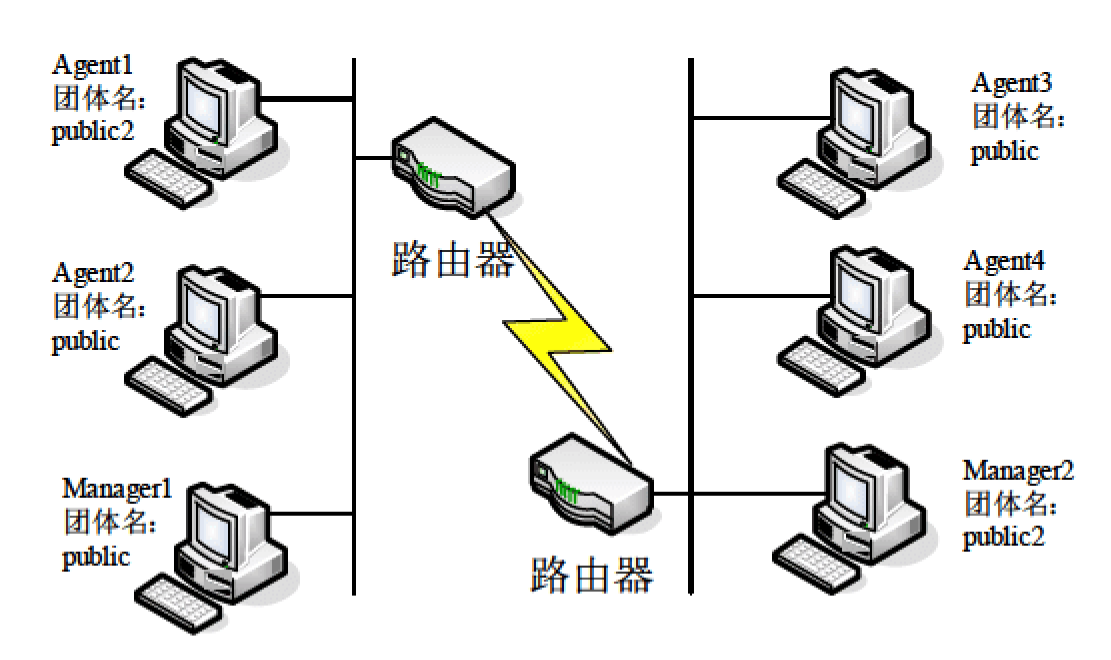
然后 ping 一台同网段计算机的 IP，如果 ping 不通则表明网络线路出现故障。

参考答案

（47）C

试题（48）、（49）

SNMP 代理使用__（48）__操作向管理端通报重要事件的发生。在下图中，__（49）__能够响应 Manager2 的 getRequest 请求。



（48）A. GetRequest　B. Get-nextRequest　C. SetRequest　D. Trap

（49）A. Agent1　B. Agent2　C. Agent3　D. Agent4

试题（48）、（49）分析

本题考查的是 SNMP 的知识。

试题（48）分析：SNMP 实体不需要在发出请求后等待响应到来，是一个异步的请求/响应协议。SNMP 仅支持对管理对象值的检索和修改等简单操作，具体讲，SNMP 支持 4 种操作：

get：用于获取特定对象的值，提取指定的网络管理信息；

get-next：通过遍历 MIB 树获取对象的值，提供扫描 MIB 树和依次检索数据的方法；

set：用于修改对象的值，对管理信息进行控制；

trap：用于通报重要事件的发生，代理使用它发送非请求性通知给一个或多个预配置的管理工作站，用于向管理者报告管理对象的状态变化。

以上 4 个操作中，前 3 个是请求由管理者发给代理，需要代理发出响应给管理者，最后一个则是由代理发给管理者，但并不需要管理者响应。

试题（49）分析：若要确保 SNMP 服务正常运行，需要在以下几个方面做好准备工作：

（1）主机名和 IP 地址。在安装 SNMP 服务之前，对于要向其发送 SNMP 陷阱或系统中响应 SNMP 请求的主机，要确保拥有其主机名或 IP 地址。

（2）主机名解析。SNMP 服务使用一般的 Windows 主机名解析方法，将主机名解

析为 IP 地址。如果您使用主机名，一定要确保将所有相关计算机的主机名到 IP 地址的映射添加到相应的解析源（如 Hosts 文件、DNS、WINS 或 Lmhosts 文件）中。

（3）管理系统。管理系统是运行 TCP/IP 协议和第三方 SNMP 管理器软件的所有计算机。管理系统向代理请求信息。要使用 Microsoft SNMP 服务，需要至少一个管理系统。

（4）代理。SNMP 代理向管理系统提供所请求的状态信息，并报告特别事件，是一台运行 Microsoft SNMP 服务的、基于 Windows 的计算机。

（5）定义 SNMP 团体。团体是运行 SNMP 服务的主机所属的小组。团体由团体名识别。对于接收请求并启动陷阱的代理以及启动请求并接收陷阱的管理系统，使用团体名可为它们提供基本的安全和环境检查功能。代理不接受所配置团体以外的管理系统的请求。

考虑到要与多个团体的 SNMP 管理器进行通信，SNMP 代理可以同时是多个团体的成员。

如题目图所示，有两个已定义的团体：Public 和 Public2。

只有作为同一团体成员的代理和管理器才能相互通信。例如：Agent1 可以接收 Manager2 的消息并向它发送消息，因为它们都是 Public2 团体的成员；Agent2-4 可以接收 Manager1 的消息，并向它发送消息，因为它们都是默认团体 Public 的成员。

参考答案

（48）D （49）A

试题（50）

在 SNMPv2 中，一个实体接受到一个报文，一般经过 4 个步骤：

① 把 PDU 部分、源和目标端口号交给认证服务。如果认证失败，发送一个陷入，丢弃报文。

② 协议实体对 PDU 做句法检查。如果通过检查，则根据团体名和适当的访问策略作相应的处理。

③ 如果认证通过，则把 PDU 转换成 ASN.1 的形式。

④ 对报文进行语法检查，丢弃出错的报文。

这四个步骤的正确次序是__（50）__。

（50）A. （1）（3）（2）（4） B. （3）（2）（1）（4）

C. （4）（1）（3）（2） D. （2）（1）（3）（4）

试题（50）分析

本题考查的是 SNMPv2 实体接收报文的过程。

SNMPv2 实体接收到一个报文要经过以下过程：

① 对报文进行语法检查，丢弃出错的报文；

② 把 PDU 部分、源和目标端口号交给认证服务。如果认证失败，发送一个陷入，丢弃报文；

③ 如果认证通过，则把 PDU 转换成 ASN.1 的形式；

④ 协议实体对 PDU 做句法检查，如果通过，根据团体名和适当的访问策略作相应的处理。

参考答案

（50）C

试题（51）、（52）

以下列出的 IP 地址中，不能作为目标地址的是（51），不能作为源地址的是（52）。

（51）A．0.0.0.0　　B．127.0.0.1

C．100.10.255.255　　D．10.0.0.1

（52）A．0.0.0.0　　B．127.0.0.1

C．100.255.255.255　　D．10.0.0.1

试题（51）、（52）分析

全 0 的 IP 地址表示本地计算机，在点对点通信中不能作为目标地址。A 类地址 100.255.255.255 属于广播地址，不能作为源地址。

参考答案

（51）A　（52）C

试题（53）

私网地址用于配置本地网络，下面的地址中，属于私网地址的是（53）。

（53）A．100.0.0.0　　B．172.15.0.0

C．192.168.0.0　　D．244.0.0.0

试题（53）分析

RFC 1918标准规定了 3 种私网地址，凡是不需要连接公网的设备，都可以利用私网地址互相通信。这 3 种私网地址是：

IANA 保留的私网地址	开始范围	结束范围
The 24 比特的地址块	10.0.0.0	10.255.255.255
The 20 比特的地址块	172.16.0.0	172.31.255.255
The 16-比特的地址块	192 168.0.0	192.168.255.255

这些地址不会被路由，只能在私网中使用。如果一个使用私网地址的设备想要与外部通信，则要通过路由器将其私网地址转化为公网地址。

参考答案

（53）C

试题（54）、（55）

某公司网络的地址是 202.100.192.0/20，要把该网络分成 16 个子网，则对应的子网

掩码应该是＿（54）＿，每个子网可分配的主机地址数是＿（55）＿。

（54）A．255.255.240.0　　B．255.255.224.0
　　C．255.255.254.0　　D．255.255.255.0

（55）A．30　　B．62
　　C．254　　D．510

试题（54）、（55）分析

公司网络 202.100.192.0/20 需要 20 位子网掩码，分成 16 个子网又要增加 4 位子网掩码，总共为 24 位子网掩码，所以子网掩码为 255.255.255.0。每个子网可分配的主机数是 $2^8-2=254$。

参考答案

（54）D　（55）C

试题（56）

以下给出的地址中，不属于子网 192.168.64.0/20 的主机地址是＿（56）＿。

（56）A．192.168.78.17　　B．192.168.79.16
　　C．192.168.82.14　　D．192.168.66.15

试题（56）分析

地址 192.168.78.17 的二进制表示为：**11000000 10101000 0100**1110 00010001

地址 192.168.79.16 的二进制表示为：**11000000 10101000 0100**1111 00010000

地址 192.168.82.14 的二进制表示为：**11000000 10101000 0101**0010 00001110

地址 192.168.66.15 的二进制表示为：**11000000 10101000 0100**0010 00001111

而网络地址 192.168.64.0/20 可表示为：　**11000000 10101000 0100**0000 00000000

只有地址 192.168.82.14 的 20 位前缀不能与其匹配，所以地址 192.168.82.14 不属于子网 192.168.64.0/20。

参考答案

（56）C

试题（57）

路由器命令“Router(config)# access-list 1 permit 192.168.1.1”的含义是＿（57）＿。

（57）A．不允许源地址为 192.168.1.1 的分组通过，如果分组不匹配，则结束
　　B．允许源地址为 192.168.1.1 的分组通过，如果分组不匹配，则检查下一条语句
　　C．不允许目标地址为 192.168.1.1 的分组通过，如果分组不匹配，则结束
　　D．允许目标地址为 192.168.1.1 的分组通过，如果分组不匹配，则检查下一条语句

试题（57）分析

访问控制列表（ACL）分为标准的和扩展的两种类型。标准 ACL 只能根据分组中

的 IP 源地址进行过滤，例如可以允许或拒绝来自某个源设备的所有通信。扩展 APL 不但可以根据源地址或目标地址进行过滤，还可以根据不同的上层协议信息进行过滤。例如，可以对 PC 机与远程服务器的 Telnet 会话进行过滤。配置标准 ACL 的命令如下：

```
Router(config)# access-list ACL_# permit|deny conditions
```

ACL 编号（*ACL_#*）的作用是把 ACL 语句组合成一个列表。ACL 编号的选择有一定的取值范围，如下表所示。ACL 语句中的条件（*conditions*）表示分组中用于匹配的内容，即 IP 地址或协议信息。

ACL 类型	ACL 编号范围
IP 标准	1～99，1300～1999
标准 Vines	1～99
IP 扩展	100～199，2000～2699
扩展 Vines	100～199
网桥类型代码（第二层）	200～299
DECnet	300～399
标准 XNS	400～499
扩展 XNS	500～599
AppleTalk	600～699
网桥 MAC 地址和制造商代码	700～799
IPX 标准	800～899
IPX 扩展	900～999
IPX SAP 过滤器	1000～1099
扩展的透明网桥	1100～1199
IPX NLSP	1200～1299

题中的语句是一条标准 ACL 语句，表示允许源地址为 192.168.1.1 的分组通过，如果分组不匹配，则检查下一条语句。

参考答案

（57）B

试题（58）

路由器 Console 端口默认的数据速率为<u>（58）</u>。

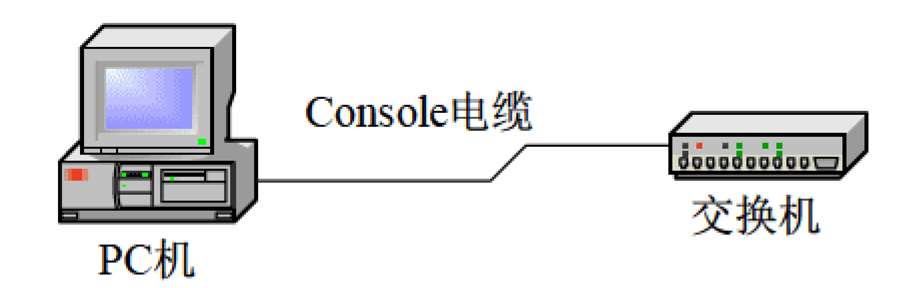
（58）A．2400b/s　　B．4800b/s

C．9600b/s　　D．10Mb/s

试题（58）分析

可以通过控制台端口来访问和配置路由器/交换机。这也是最常用、最有效的配置方法。控制台端口（Console）是路由器的基本端口，连接控制台端口的线缆称为控制台电

缆（Console Cable）。控制台电缆一端插入交换机的控制台端口，另一端插入 PC 机的串行口，从而实现对交换机的访问和控制，参见下图所示。



控制台端口默认的数据速率为 9600b/s，参见下图。



参考答案

（58）C

试题（59）

当启用 VTP 修剪功能后，如果交换端口中加入一个新的 VLAN，则立即＿（59）＿。

（59）A．剪断与周边交换机的连接

B．把新的 VLAN 中的数据发送给周边交换机

C．向周边交换机发送 VTP 连接报文

D．要求周边交换机建立同样的 VLAN

试题（59）分析

VLAN 中继协议（VLAN Trunking Protocol，VTP）用于在交换网络中简化 VLAN 的管理。VTP 协议在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文可以传播到管理域中的所有交换机。

在默认情况下，所有交换机通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包、或者一个未知的单播数据包，交换机都会将其洪泛（flood）到

所有与源 VLAN 端口相关的各个输出端口上（包括中继端口）。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动端口，则这种洪泛发送的数据包是无用的。

为了解决这个问题，可以使用静态或动态修剪的方法。所谓静态修剪，就是手工剪掉中继链路上不活动的 VLAN，在多个交换机组成多个 VLAN 的网络中，这种工作方式很容易出错，容易出现连接问题。

VTP 动态修剪允许交换机之间共享 VLAN 信息，也允许交换机从中继连接上动态地剪掉不活动的 VLAN，使得所有共享的 VLAN 都是活动的。例如，交换机 A 告诉交换机 B，它有两个活动的 VLAN1 和 VLAN2，而交换机 B 告诉交换机 A，它只有一个活动的 VLAN1，于是，它们就共享这样的事实：VLAN 2 在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。这样做的好处是显而易见的，如果在交换机 B 上添加了 VLAN 2 的成员，交换机 B 就会通知交换机 A，它有了一个新的活动的 VLAN 2，于是，两个交换机动态地把 VLAN 2 添加到它们之间的中继链路配置中。

参考答案

（59）C

试题（60）、（61）

下面是显示交换机端口状态的例子：

```
2950# show interface fastEthernet0/1 switchport
Name: fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1,2
Pruning VLANs Enabled: 2-1001
Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
```

在以上显示的信息中，端口 fa0/1 的链路模式被设置为<u>（60）</u>，默认的 VLAN 为<u>（61）</u>。

（60）A．中继连接状态，并要求对方也建立中继连接

B．中继连接状态，不要求与对方建立中继连接

C．接入链路状态，要求与对方建立中继连接

D．接入链路状态，不要求对方建立中继连接

（61）A．VLAN0　　B．VLAN1

C．VLAN2　　D．VLAN3

试题（60）、（61）分析

从以上信息的第 4 和第 5 行

```
Administrative mode: trunk
Operational Mode: trunk
```

以及第 8 行

```
Negotiation of Trunking: Disabled
```

可知交换机端口处于中继连接状态，不要求与对方建立中继连接。从第 10 行

```
Trunking Native Mode VLAN: 1 (default)
```

可知默认的 VLAN 为 VLAN1。

参考答案

（60）B　（61）B

试题（62）

以太网的 CSMA/CD 协议采用坚持型监听算法。与其他监听算法相比，这种算法的主要特点是 __（62）__。

（62）A．传输介质利用率低，冲突概率也低

B．传输介质利用率高，冲突概率也高

C．传输介质利用率低，但冲突概率高

D．传输介质利用率高，但冲突概率低

试题（62）分析

以太网可以采用以下三种监听算法：

（1）非坚持型监听算法：当一个站准备好帧，发送之前先监听信道。

① 若信道空闲，立即发送，否则转 2；

② 若信道忙，则后退一个随机时间，重复 1。

由于随机时延后退，从而减少了冲突的概率；然而，可能出现的问题是因为后退而使信道闲置一段时间，这使信道的利用率降低，而且增加了发送时延。

（2）1-坚持型监听算法：当一个站准备好帧，发送之前先监听信道，

① 若信道空闲，立即发送，否则转 2；

② 若信道忙，继续监听，直到信道空闲后立即发送。

这种算法的优缺点与前一种正好相反：有利于抢占信道，减少信道空闲时间；但是多个站同时都在监听信道时必然发生冲突。

（3）P-坚持型监听算法。这种算法汲取了以上两种算法的优点，但较为复杂。这种算法是：

① 若信道空闲，以概率 P 发送，以概率（1-P）延迟一个时间单位。一个时间单位等于网络传输时延τ；

② 若信道忙，继续监听直到信道空闲，转 1；

③ 如果发送延迟一个时间单位τ，则重复 1。

困难的问题是决定概率 P 的值，P 的取值应在重负载下能使网络有效地工作。为了说明 P 的取值对网络性能的影响，我们假设有 n 个站正在等待发送，与此同时，有一个站正在发送。当这个站发送停止时，实际要发送的站数等于 nP。若 nP 大于 1，则必有多个站同时发送，这必然会发生冲突。这些站感觉到冲突后若重新发送，就会再一次发生冲突。更糟的是有的站还可能产生新帧，与这些未发出的帧竞争，更加剧了网上的冲突。极端情况下会使网络吞吐率下降到 0。若要避免这种灾难，对于某种 n 的峰值，nP 必须小于 1。然而若 P 值太小，发送站就要等待较长的时间。在轻负载的情况下，这意味着较大的发送时延。例如，只有一个站有帧要发送，若 P=0.1，则以上算法的第 1 步重复的平均次数为 1/P=10，也就是说这个站平均多等待 9 倍的时间单位τ。

以太网的 CSMA/CD 协议采用坚持型监听算法。根据以上分析可知，答案 B 是正确的。

参考答案

（62）B

试题（63）

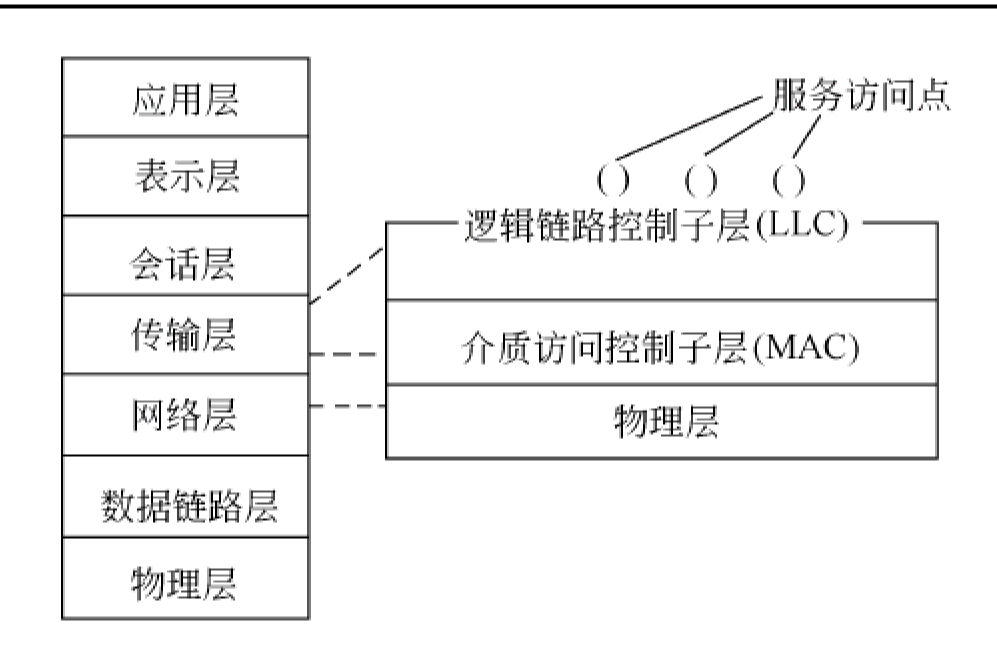
IEEE 802 局域网中的地址分为两级，其中 LLC 地址是__（63）__。

（63）A．应用层地址　　　　B．上层协议实体的地址

　　　C．主机的地址　　　　D．网卡的地址

试题（63）分析

由于局域网是分组广播式网络，网络层的路由功能是不需要的，所以在 IEEE802 标准中，网络层简化成了上层协议的服务访问点 SAP。又由于局域网使用多种传输介质，而介质访问控制协议与具体的传输介质和拓扑结构有关，所以 IEEE802 标准把数据链路层划分成了两个子层。与物理介质相关的部分叫做介质访问控制 MAC（Media Access Control）子层，与物理介质无关的部分叫做逻辑链路控制 LLC（Logical Access Control）子层。LLC 提供标准的 OSI 数据链路层服务，这使得任何高层协议（例如 TCP/IP，SNA 或有关的 OSI 标准）都可运行于局域网标准之上。局域网的物理层规定了传输介质及其接口的电气特性，机械特性，接口电路的功能以及信令方式和信号速率等。整个局域网的标准以及与 OSI 参考模型的对应关系如下图所示：



参考答案

（63）B

试题（64）

快速以太网物理层规范 100BASE-TX 规定使用（64）。

（64）A．1 对 5 类 UTP，支持 10M/100M 自动协商

B．1 对 5 类 UTP，不支持 10M/100M 自动协商

C．2 对 5 类 UTP，支持 10M/100M 自动协商

D．2 对 5 类 UTP，不支持 10M/100M 自动协商

试题（64）分析

1995 年 100Mb/s 的快速以太网标准 IEEE 802.3u 正式颁布，这是基于 10Base-T 和 10Base-F 技术、在基本布线系统不变的情况下开发的高速局域网标准。快速以太网使用的传输介质如下表所示，其中多模光纤的芯线直径为 62.5μm，包层直径为 125μm，单模光线芯线直径为 8μm，包层直径也是 125μm。

标　准	传输介质	特性阻抗	最大段长
100Base-TX	2 对 5 类 UTP	100Ω	100m
	2 对 STP	150Ω	
100Base-FX	一对多模光纤 MMF	62.5/125μm	2km
	一对单模光纤 SMF	8/125μm	40km
100Base-T4	4 对 3 类 UTP	100Ω	100m
100Base-T2	2 对 3 类 UTP	100Ω	100m

参考答案

（64）C

试题（65）、（66）

IEEE802.11 定义了无线局域网的两种工作模式，其中的（65）模式是一种点对点连接的网络，不需要无线接入点和有线网络的支持。IEEE802.11g 的物理层采用了扩频技

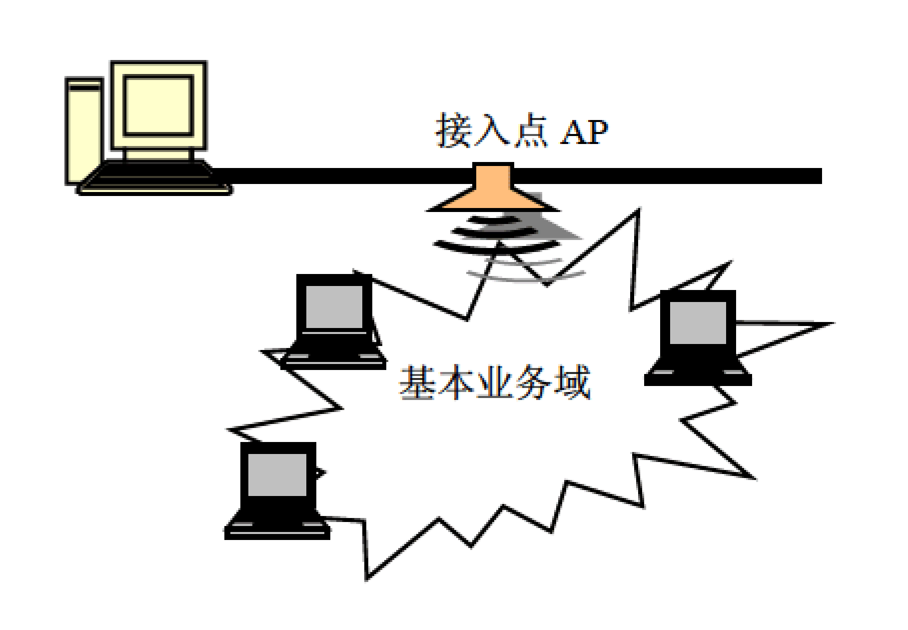
术，工作在<u>（66）</u>频段。

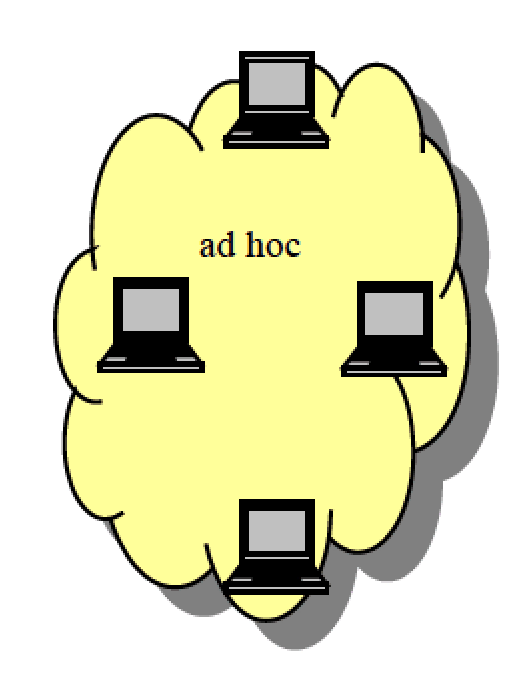
（65）A．Roaming　　B．Ad Hoc
　　C．Infrastructure　　D．DiffuseIR

（66）A．600MHz　　B．800MHz
　　C．2.4GHz　　D．19.2GHz

试题（65）、（66）分析

IEEE802.11 标准定义了两种无线网络的拓扑结构，一种是基础设施网络（Infrastructure Networking），另一种是特殊网络（Ad Hoc Networking），参见下图。在基础设施网络中，无线终端通过接入点（Access Point，AP）访问骨干网设备，或者互相访问。接入点如同一个网桥，它负责在 802.11 和 802.3MAC 协议之间进行转换。





Ad hoc 网络是一种点对点连接，不需要有线网络和接入点的支持，以无线网卡连接的终端设备之间可以直接通信。这种拓扑结构适合在移动情况下快速部署网络，主要用在军事领域，也可以用在商业领域进行语音和数据传输。802.11 支持单跳的 Ad hoc 网络，当一个无线终端接入时首先寻找来自 AP 或其他终端的信标信号，如果找到了信标，则 AP 或其他终端就宣布新的终端加入了网络；如果没有检测到信标，该终端就自行宣布存在于网络之中。

IEEE802.11 委员会相继制定了多种物理层标准。1997 年颁布的 IEEE802.11 标准运行在 2.4GHz 的 ISM（Industrial Scientific and Medical）频段，采用扩频通信技术，支持 1Mb/s 和 2Mb/s 数据速率。随后又出现了两个新的标准，1998 年推出的 IEEE802.11b 标准也是运行在 ISM 频段，采用 CCK（Complementary Code Keying）技术，支持 11Mb/s 的数据速率。1999 年推出的 IEEE802.11a 标准运行在 U-NII（Unlicensed National Information Infrastructure）频段，采用 OFDM（Orthogonal Frequency Division Multiplexing）调制技术，支持最高达 54Mb/s 的数据速率。目前的 WLAN 标准主要有 4 种，如下表：

名　　称	发 布 时 间	工 作 频 段	调 制 技 术	数 据 速 率
802.11	1997 年	2.4GHz ISM 频段	DBPSK	1Mb/s
			DQPSK	2Mb/s
802.11b	1998 年	2.4GHz ISM 频段	CCK	5.5Mb/s，11Mb/s
802.11a	1999 年	5GHz U-NII 频段	OFDM	54Mb/s
802.11g	2003 年	2.4GHz ISM 频段	OFDM	54Mb/s

参考答案

（65）B　（66）C

试题（67）

以下关于网络存储描述正确的是__（67）__。

（67）A．SAN 系统是将存储设备连接到现有的网络上，其扩展能力有限

B．SAN 系统是将存储设备连接到现有的网络上，其扩展能力很强

C．SAN 系统使用专用网络，其扩展能力有限

D．SAN 系统使用专用网络，其扩展能力很强

试题（67）分析

本题考查的是网络存储的概念。

存储区域网络（Storage Area Network， SAN）是一种专用网络，可以把一个或多个系统连接到存储设备和子系统。SAN 可以被看作是负责存储传输的“后端”网络，而“前端”网络（或称数据网络）负责正常的 TCP/IP 传输。

与 NAS 相比，SAN 具有下面几个特点。

（1）SAN 具有无限的扩展能力。

由于 SAN 采用了网络结构，服务器可以访问存储网络上的任何一个存储设备，因此用户可以自由增加磁盘阵列、带库和服务器等设备，使得整个系统的存储空间和处理能力得以按客户需求不断扩大。

（2）SAN 具有更高的连接速度和处理能力。

参考答案

（67）D

试题（68）

__（68）__是错误的网络设备选型原则。

（68）A．选择网络设备，应尽可能地选择同一厂家的产品

B．为了保证网络性能，尽可能地选择性能高的产品

C．核心设备的选取要考虑系统日后的扩展性

D．网络设备选择要充分考虑其可靠性

试题（68）分析

本题考查的是网络设备选型原则。

网络设备选型应遵守以下原则：

（1）实用性原则

计算机设备、服务器设备和网络设备在技术性能逐步提升的同时，其价格却在逐年下降。因此，不可能也没必要实现所谓“一步到位”。所以，网络方案设计中应把握“够用”和“实用”原则。网络系统应采用成熟可靠的技术和设备，达到实用、经济和有效的目的。

（2）高可用性/可靠性原则

对于像证券、金融、铁路和民航等行业的网络系统应确保很高的平均无故障时间和尽可能低的平均故障率。在这些行业的网络方案设计中，高可用性和系统可靠性应优先考虑。

（3）可扩展性原则

网络总体设计不仅要考虑到近期目标，也要为网络的进一步发展留有扩展的余地。因此，需要统一规划和设计。网络系统应在规模和性能两方面具有良好的可扩展性。由于目前网络产品标准化程度较高，因此可扩展性要求基本不成问题。

（4）易用性原则

整个网络设备必须易于管理、安装和使用，在可能的情况下，应尽可能地选择同一厂家的产品。

参考答案

（68）B

试题（69）

下面关于网络工程需求分析的论述中，正确的是（69）。

（69）A．任何网络都不可能是一个能够满足各项功能需求的万能网

B．必须采用最先进的网络设备，获得最高的网络性能

C．网络需求分析独立于应用系统的需求分析

D．网络需求分析时可以先不考虑系统的扩展性

试题（69）分析

本题考查的是网络工程需求分析中的基本问题。在网络需求分析中应该注意使系统能满足用户对应用处理不同程度的需求，以及逐步升级的发展规划，以节约投资避免系统性能的闲置和浪费，设计上必须重视网络的拓展能力。网络的拓展包括：

① 网络规模的扩展，包括网络的地理分布，用户数量的不断增加。

② 应用内容的扩展，IP 主干网络不仅担负数据传输的任务，包括其他视频和语音服务也会不断的增加到 IP 网络中去，这就要求主干网络设计必支持多种业务。

③ 网络容量的扩展，随着规模和应用的拓展网络的传输容量也必须能相应的增加。

因此，任何网络都不可能是一个能够满足各项功能需求的万能网，在需求分析阶段必需认真考虑与规划。

参考答案

（69）A

试题（70）

关于项目管理甘特图的结构，下列选项中合理的是 __（70）__。

（70）A．任务名称，工期，开始时间，前置任务，后置任务，资源名称

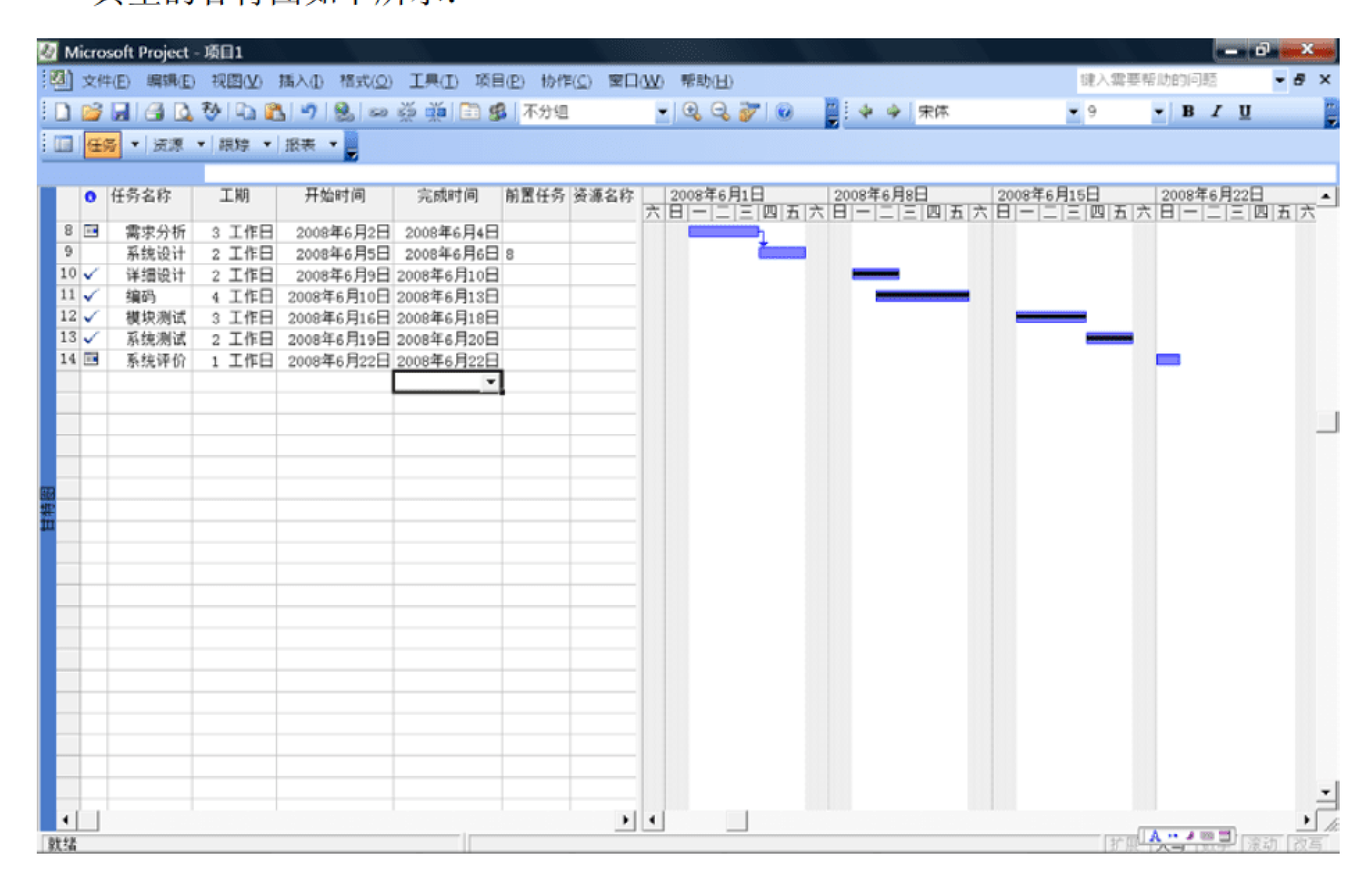
B．任务名称，开始时间，完成时间，后置任务，人力资源，进度线

C．任务名称，工期，开始时间，完成时间，前置任务，资源名称，进度线

D．任务名称，开始时间，完成时间，前置任务，人力资源，进度线

试题（70）分析

典型的甘特图如下所示：



参考答案

（70）C

试题（71）～（75）

WLANs are increasingly popular because they enable cost-effective connections among people and applications that were not possible in the past. For example, WLAN-based applications can enable fine-grained management of supply __（71）__ to improve their efficiency and reduce __（72）__. WLANs can also enable entirely new business processes. To cite but one example, hospitals are using WLAN-enabled point-of-care __（73）__ to reduce errors and

improve overall patient care. WLAN management solutions provide a variety of other benefits that can be substantial but difficult to measure. For example, they can protect corporate data by preventing （74） through rogue access points. They can improve overall network management by integrating with customers' existing systems. Fortunately, it isn't necessary to measure these benefits to justify investing in WLAN management solutions, which can quickly pay for themselves simply by minimizing time-（75） deployment and administrative chores.

（71）A. custom　B. server　C. chains　D. chances

（72）A. overhead　B. connection　C. supply　D. effect

（73）A. transportations　B. applications　C. connections　D. translations

（74）A. integration　B. interest　C. instruction　D. intrusion

（75）A. capable　B. consuming　C. effective　D. connected

参考译文

无线局域网（WLAN）日益普及起来，这是因为它能够在用户和应用之间有效地建立连接，这在过去是难以做到的。例如基于 WALN 的应用可以对供应链进行细粒度的管理，从而改进效率，减少开销。WLAN 也可以创造全新的商业过程。仅举出其中的一个例子，医院使用基于 WLAN 的护理点应用来减少差错，全面改进病员护理。WLAN 管理解决方案提供的各种实质上的好处是很难度量的。例如，它可以保护公司的数据，防止恶意的访问。它可以全面地改进网络管理，并集成到用户现有的系统中。幸好，我们无需量化这些收益来证明 WLAN 管理解决方案的合理性，因为它能很快地补偿由于部署这些应用和管理事务而付出的时间开销。

参考答案

（71）C　（72）A　（73）B　（74）D　（75）B

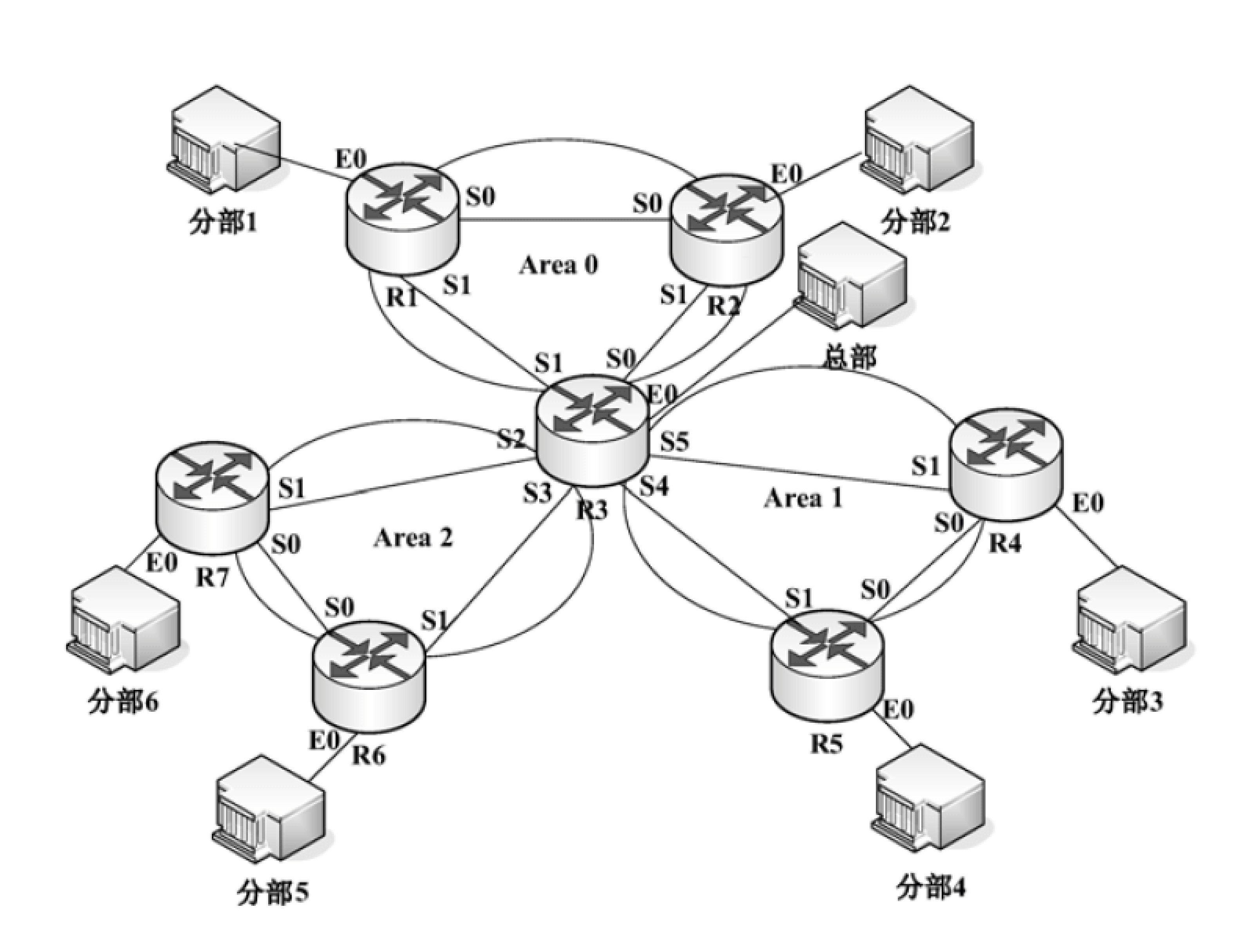
第 16 章　2008 上半年网络工程师下午试题分析与解答

试题一（15 分）

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

某单位有 1 个总部和 6 个分部，各个部门都有自己的局域网。该单位申请了 6 个 C 类 IP 地址 202.115.10.0/24～202.115.15.0/24，其中总部与分部 4 共用一个 C 类地址。现计划将这些部门用路由器互联，网络拓扑结构如下图所示。



【问题 1】

该网络采用 R1～R7 共 7 台路由器，采用动态路由协议 OSPF。由图 1-1 可见，该网络共划分了 3 个 OSPF 区域，其主干区域为<u>（1）</u>，主干区域中，<u>（2）</u>为区域边界路由器，<u>（3）</u>为区域内路由器。

【问题 2】

下表是该系统中路由器的 IP 地址分配表。

路由器	端口 IP 地址	路由器	端口 IP 地址	路由器	端口 IP 地址
R1	E0：202.115.10.1/24	R4	E0：202.115.12.1/24	R6	E0：202.115.14.1/24
	S0：10.0.0.1/24		S0：10.0.3.2/24		S0：10.0.6.1/24
	S1：10.0.1.1/24		S1：10.0.5.1/24		S1：10.0.7.1/24
R2	E0：202.115.11.1/24	R5	E0：202.115.13.1/25	R7	E0：202.115.15.1/24
	S0：10.0.0.2/24		S0：10.0.3.1/24		S0：10.0.6.2/24
	S1：10.0.2.1/24		S1：10.0.4.1/24		S1：10.0.8.1/24

请根据上图完成以下 R3 路由器的配置：

R3 (config)#interface e0/1　　（进入接口 e0/1 配置模式）
R3 (config-if)#ip address 202.115.13.254 ___（4）___　　（设置 IP 地址和掩码）
R3(config) # interface s0/0　　（进入串口配置模式）
R3(config-if) #ip address ___（5）___ 255.255.255.0　　（设置 IP 地址和掩码）
R3(config) # interface s0/1
R3(config-if) #ip address ___（6）___ 255.255.255.0
R3(config) # interface s0/2
R3(config-if) #ip address ___（7）___ 255.255.255.0
R3(config) # interface s0/3
R3(config-if) #ip address ___（8）___ 255.255.255.0
R3(config) # interface s0/4
R3(config-if) #ip address ___（9）___ 255.255.255.0
R3(config) # interface s0/5
R3(config-if) #ip address ___（10）___ 255.255.255.0

【问题 3】

该单位部门 4 共有 110 台 PC 机，通过交换机连接路由器 R5 接入网络。其中一台 PC 机 IP 地址为 202.115.13.5，则其子网掩码应为___（11）___，网关地址应为___（12）___。

试题一分析

本题目考查的是 OSPF 配置问题。OSPF（Open Shortest Path First 开放式最短路径优先）是一个内部网关协议（Interior Gateway Protocol,简称 IGP），用于在单一自治系统（autonomous system，AS）内决策路由。与 RIP 相对，OSPF 是链路状态路由协议，而 RIP 是距离向量路由协议。

【问题 1】

本问题考查的是 OSPF 区域问题。OSPF 网络为了降低区域内工作路由的负担，将整个 OSPF 区域分为以下 2 个级别的层次：主干区域和非主干区域。

在一个 OSPF 区域中只能有一个主干区域，可以有多个非主干区域。主干区域的区域号为 0。各非主干区域间是不可以交换信息的，他们只有与主干区域相连，通过主干

区域相互交换信息。

非主干区域和主干区域之间相连的路由叫区域边界路由，在区域边界路由器中记载了各区域的所有路由表。各非主干区域内中的路由器称为区域内路由器，在区域内路由器中只记载了本区域内的路由表。

由本题示意图可见，该系统分为 Area 0、Area 1、Area 2 三个区域，其中 Area 0 为主干区域，Area 1、Area 2 为非主干区域，在主干区域中有 R1、R2、R3 三个路由器，其中 R3 为区域边界路由器，R2、R3 为区域内路由器。

【问题 2】

本问题考查的是路由器 IP 地址分配问题。

由本题示意图所示，R3 路由器的 E0 口是连接总部的以太网口。从题目可知，总部与分部 4 共用一个 C 类地址，通过表 1-1 可知分部 4 的 E0 口 IP 地址配置为 202.115.13.1/25，故 R3 路由器的 E0 口应在 202.115.13.0 网段，其子网掩码为 25 位（255.255.255.128）。

R3 的 S0 口连接的是 R2 的 S1 口，由本题表中可知，R2 的 S1 口 IP 地址配置为 10.0.2.1/24，所以 R3 的 S0 口的 IP 地址应配置为 10.0.2.2～10.0.2.254 之间任意一个地址。

R3 其余接口的配置可参照 S0 口的配置。

【问题 3】

部门 4 共有 110 台 PC 机，通过交换机连接路由器 R5 接入网络。根据本题表中可知，R5 的 E0IP 地址配置为 202.115.13.1/25，故其中 PC 机 IP 地址为 202.115.13.5 时，其子网掩码为 255.255.255.128，网关为 202.115.13.1。

参考答案

【问题 1】

（1）Area 0

（2）R3

（3）R1 和 R2

【问题 2】

（4）255.255.255.128

（5）10.0.2.2～10.0.2.254 之间任意一个地址

（6）10.0.1.2～10.0.1.254 之间任意一个地址

（7）10.0.8.2～10.0.8.254 之间任意一个地址

（8）10.0.7.2～10.0.7.254 之间任意一个地址

（9）10.0.4.2～10.0.4.254 之间任意一个地址

（10）10.0.5.2～10.0.5.254 之间任意一个地址

【问题 3】

（11）255.255.255.128

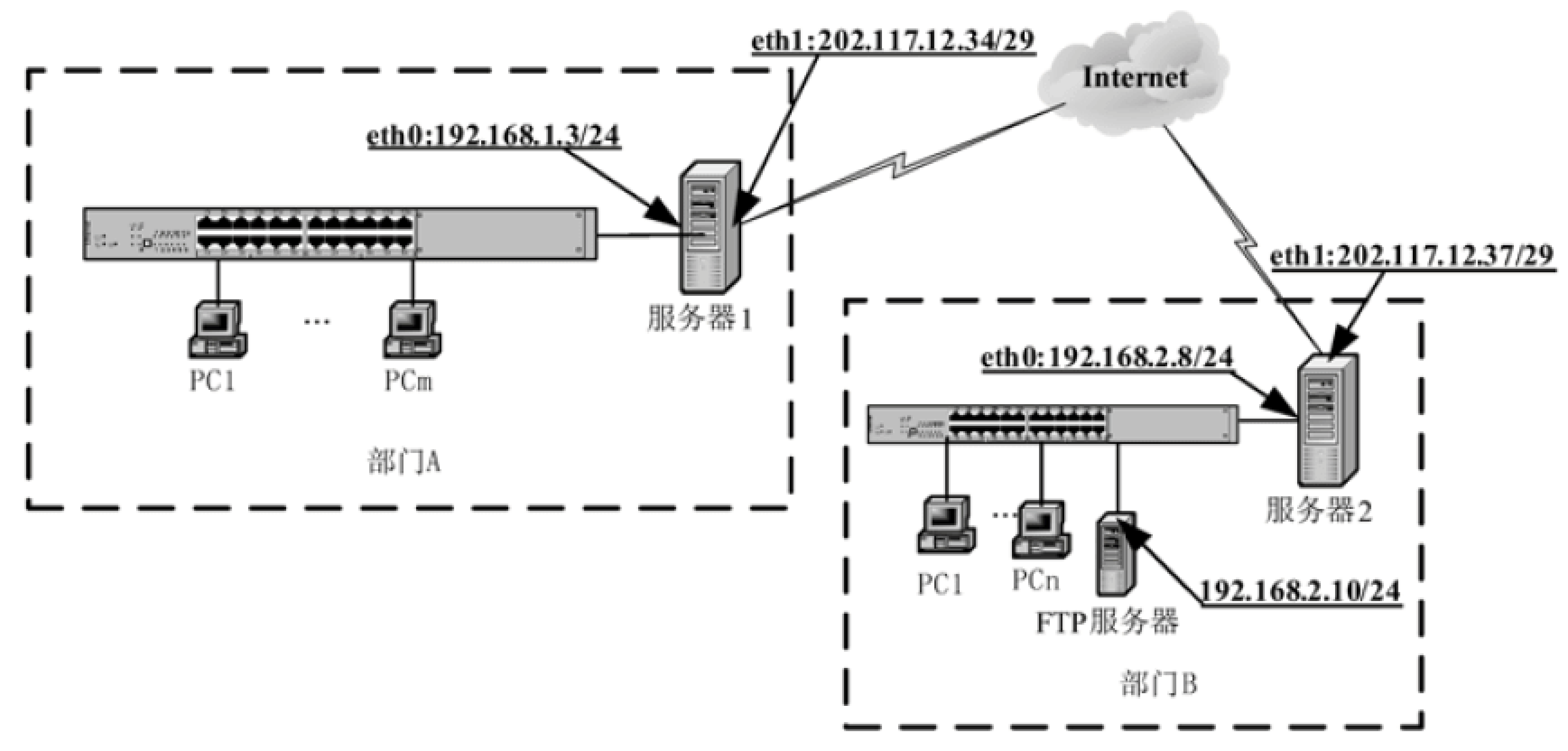
（12）202.115.13.1

试题二（15 分）

阅读下列说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。

【说明】

某公司的两个部门均采用 Windows 2003 的 NAT 功能共享宽带连接访问 Internet，其网络结构和相关参数如下图所示。ISP 为该公司分配的公网 IP 地址段为 202.117.12.32/29。



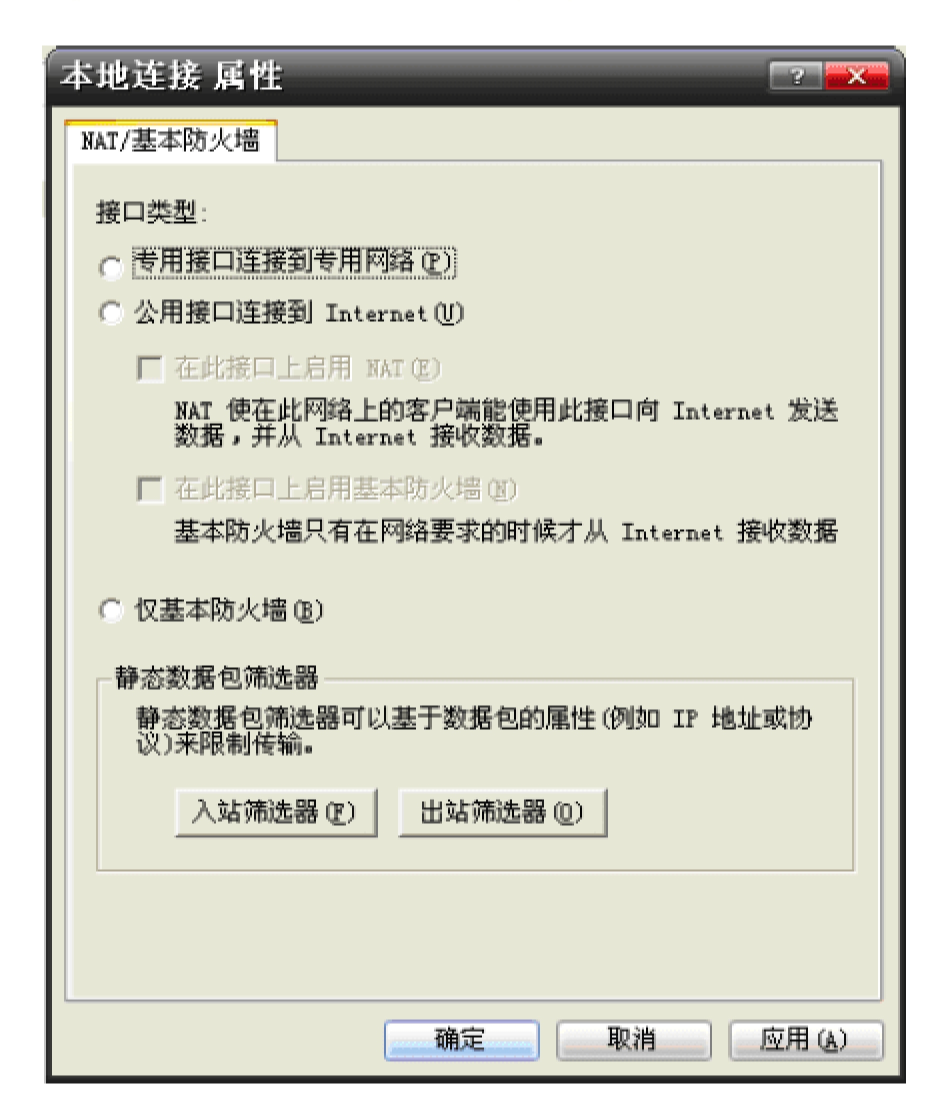
【问题 1】

在 Windows 2003 中，＿（1）＿不能实现 NAT 功能。

备选答案：

A. 终端服务管理器　　B. Internet 连接共享　　C. 路由和远程访问





【问题 2】

在上页左上图所示的窗口中，为部门 B 的服务器 2 配置“路由和远程访问”功能，新增 eth0 和 eth1 上的网络连接。eth0 上的网络连接应该选中右上图中的 (2) 选项进行配置，eth1 上的网络连接应该选中右上图中的 (3) 选项进行配置。

(2)、(3) 备选答案：

A. 专用接口连接到专用网络

B. 公用接口连接到 Internet

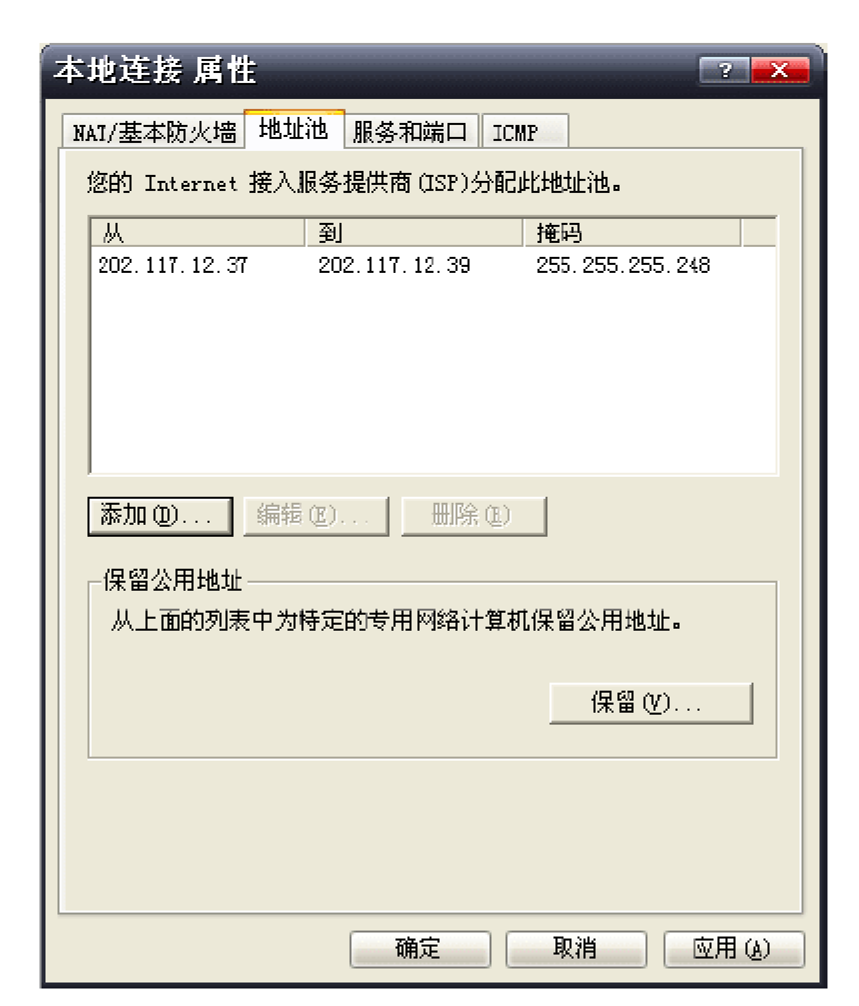
C. 仅基本防火墙

【问题 3】

部门 B 中主机 PC1 的默认网关地址应配置为 (4) 才能访问 Internet。

【问题 4】

在部门 B 的服务器 2 中，如果将 ISP 分配的可用公网 IP 地址添加到地址池（如左下图所示），那么服务器 1 收到来自部门 B 的数据包的源地址可能是 (5) 。如果部门 B 中两台不同 PC 机同时发往公网的两个数据包的源地址相同，则它们通过 (6) 相互区分。





【问题 5】

在服务器 2 的 eth1 上启用基本防火墙，如果希望将 202.117.12.38 固定分配给 IP 地址为 192.168.2.10 的 FTP 服务器，且使得公网中主机可以访问部门 B 中的 FTP 服务，应该在左上图和右上图所示的对话框中如何配置？

【问题 6】

为了实现部门 A 和部门 B 中主机互相通信，在服务器 1 和服务器 2 上都运行了“路由和远程访问”服务，在下图所示的对话框中，两台服务器的静态路由信息应配置为：

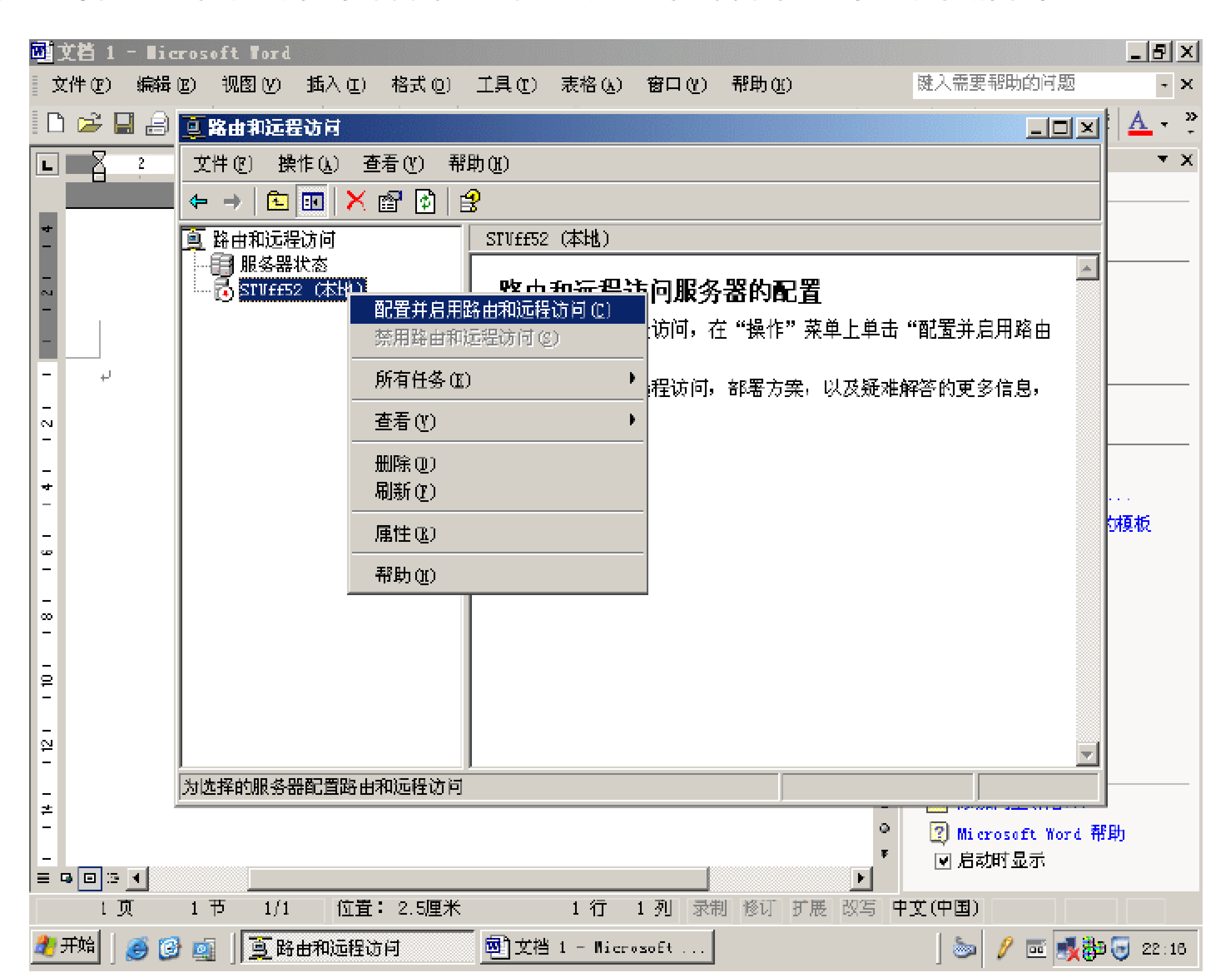
主机	接口	目标	网络掩码	网关	跃点数
服务器 1	WAN 连接	(7)	(8)	(9)	1
服务器 2	WAN 连接	(10)	(11)	(12)	1



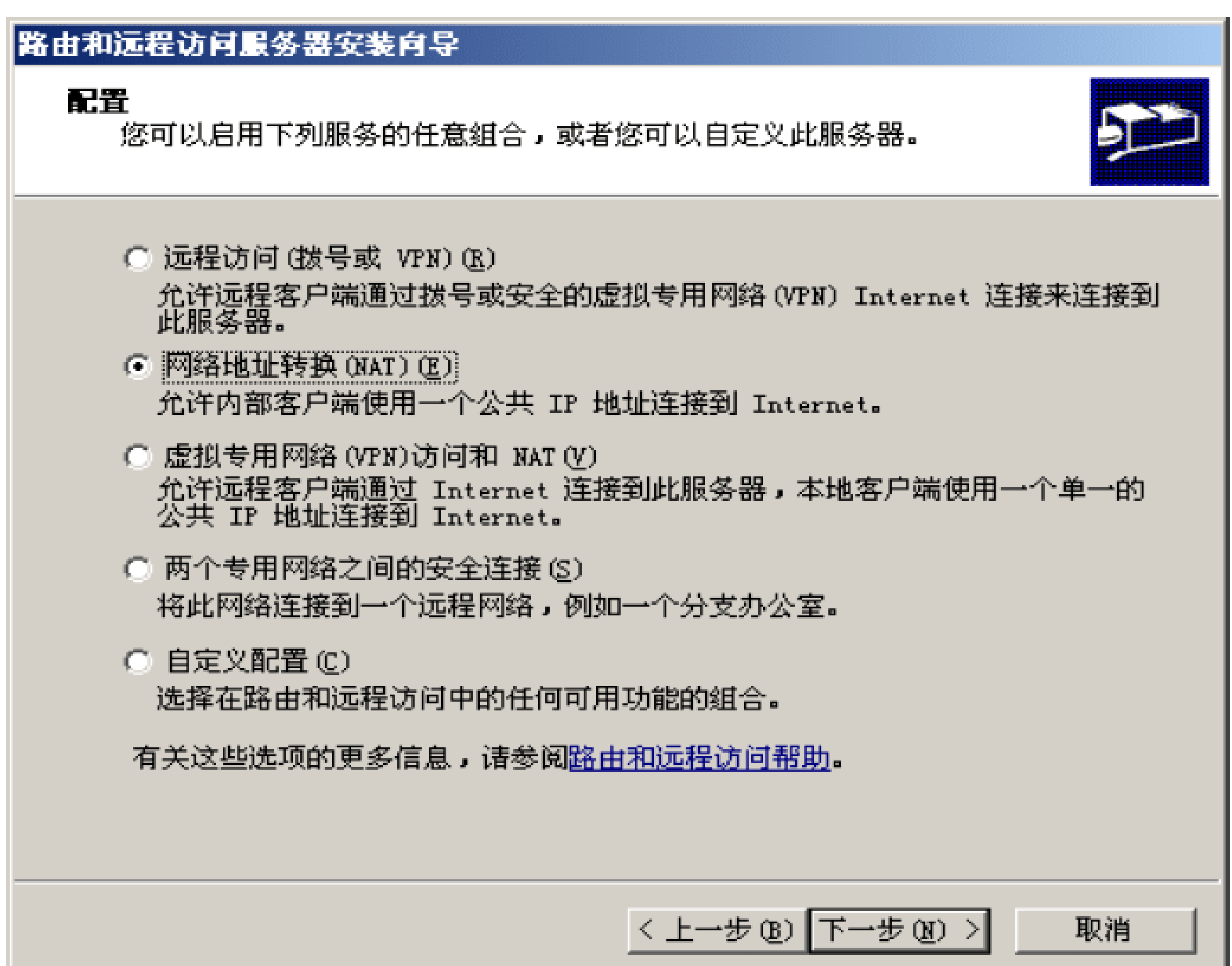
试题二分析

运行 Windows 2003 Server/Advance Server 作为微软网络新产品的核心，具有强大的网络管理服务功能，我们可以直接利用它们内置的路由服务功能实现局域网的共享上网，而不是使用所搭载的 ICS（共享网上功能）。对于使用模拟局域网网卡的 Enternet 系统下可以轻松实现，专线方式 ADSL 与此类似。首先以 Administrator 管理员身份进入服务器。

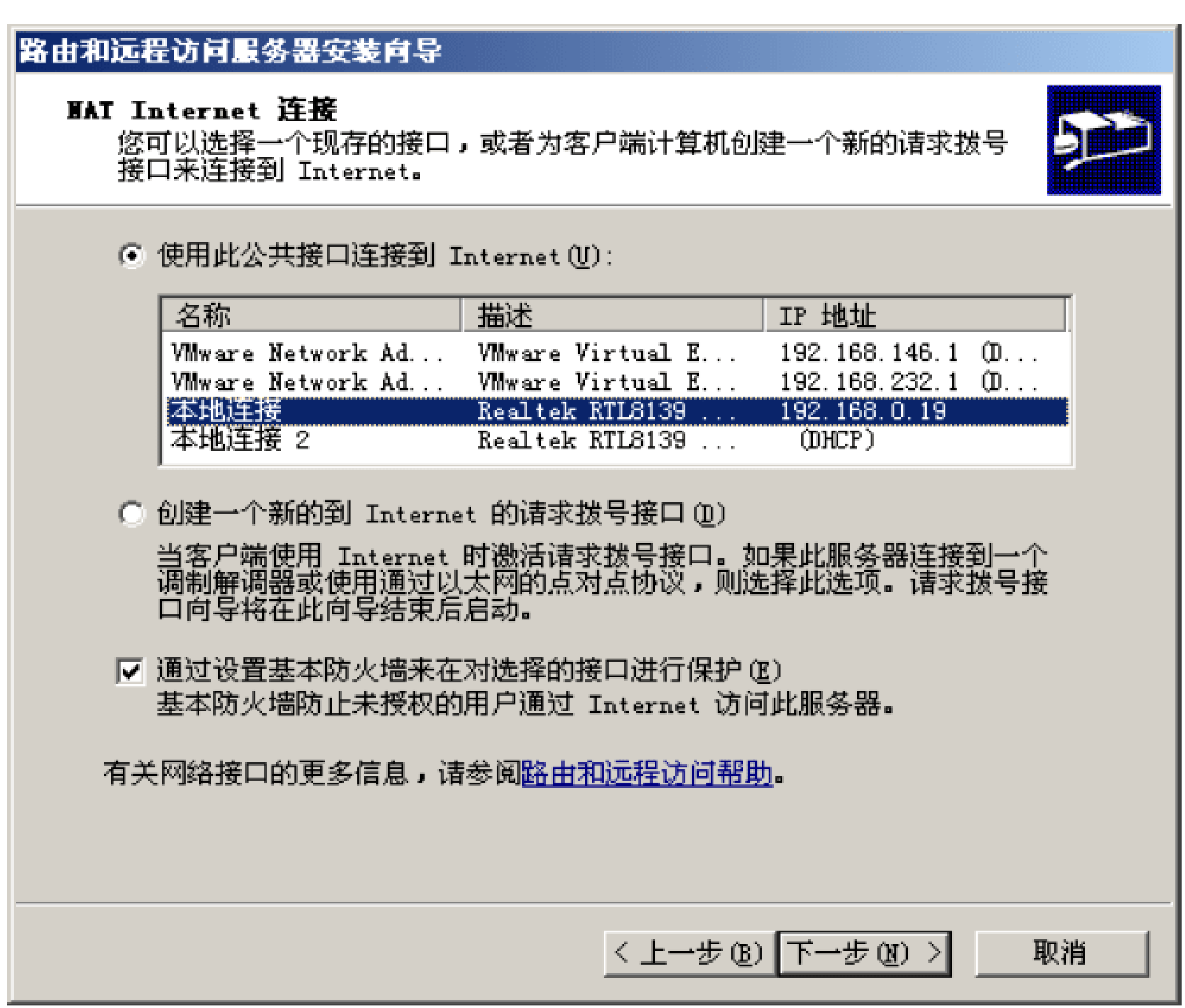
（1）从“管理工具”菜单打开“路由和远程访问”，如下图所示。



（2）进入“路由和远程访问”控制台以后，选择“网络地址转换（NAT）”，如下图所示。



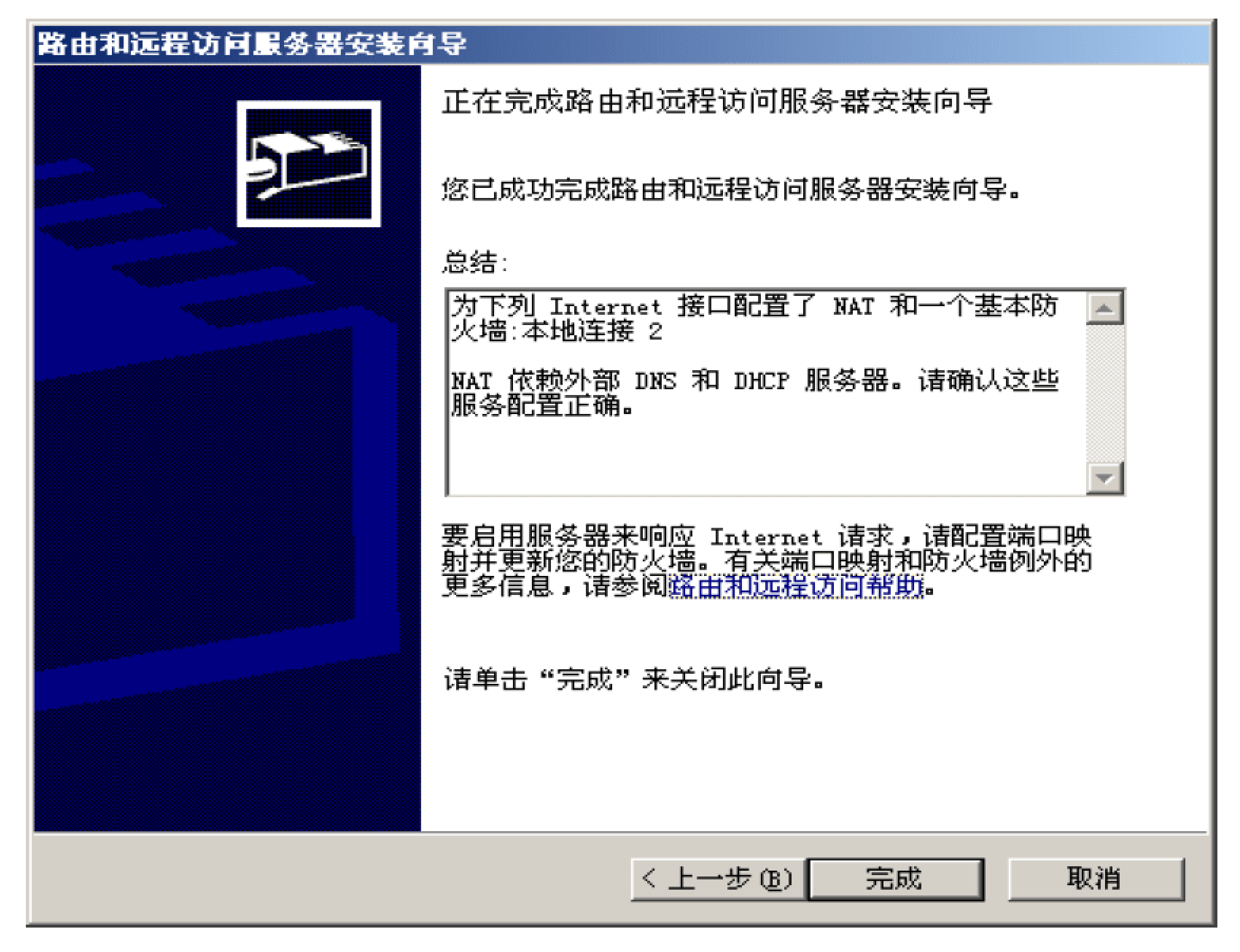
（3）然后进入配置向导界面，单击“下一步”按钮，选择“公共接口”菜单，如下图所示。



（4）然后向导将让我们选择内部接口。如下图所示。



（5）完成后如下图所示：



成功设置以后可以在控制台看到“网络地址转换（NAT）”，里面定义了内部连接和外部连接的接口，查看属性可以确认是否选择了正确的接口。

服务器设置完成以后，需要对局域网内客户机进行设置。设置方法也很简单，把网关和 NDS 都要设置成指向 Windows 2003 Server。

参考答案

【问题 1】

（1）A. 终端服务管理器

【问题 2】

（2）A. 专用接口连接到专用网络

（3）B. 公用接口连接到 Internet

【问题 3】

（4）192.168.2.8

【问题 4】

（5）202.117.12.37 或 202.117.12.38

（6）端口号

【问题 5】

在“本地连接”属性对话框中单击“保留…”按钮，在弹出的对话框中单击“添加”按钮，出现“添加保留区”对话框，依次填入 IP 地址 202.117.12.38 和 192.168.1.3，然后选中“允许会话传入到此地址”，单击“确定”按钮。然后在“本地连接属性”对话框的“服务和端口”选项卡内选中“FTP 服务”即可。

【问题 6】

（7）192.168.2.0

（8）255.255.255.0

（9）202.117.12.37

（10）192.168.1.0

（11）255.255.255.0

（12）202.117.12.34

试题三（15 分）

阅读以下关于在 Linux 系统中配置 Apache 服务器的说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

在 Linux 系统中采用 Apache 配置 Web 服务器。Apache 服务器提供了丰富的功能，包括：目录索引、目录别名、虚拟主机、HTTP 日志报告、CGI 程序的 SetUID 执行等。

【问题 1】

请在（1）、（2）、（3）、（4）空白处填写恰当的内容。

Web 客户机与服务器共同遵守＿（1）＿协议，其工作过程是：Web 客户端程序根据输入的＿（2）＿连接到相应的 Web 服务器上，并获得指定的 Web 文档。动态网页以＿（3）＿

程序的形式在服务器端处理，并给客户端返回＿（4）＿格式的文件。

（1）～（4）的备选项

A. HTML	B. ASP	C. JSP	D. IIS
E. SOAP	F. URL	G. HTTP	H. VGA

【问题 2】

请在（5）～（11）空白处填写恰当的内容。

Apache 的主配置文件为 httpd.conf。某 Web 服务器的 httpd.conf 文件部分内容如下：

```
ServerType standalone
ServerRoot "/etc/httpd"
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
MinSpareServers 5
MaxSpareServers 20
StartServers 8
MaxClients 150
MaxRequestsPerChild 100
Port 8080
User nobody
Group nobody
ServerAdmin root@webtest.com.cn
ServerName WebTest
DocumentRoot "/home/webtest/jakarta-tomcat/webapps/webtest"
Options FollowSymLinks
AllowOverride None
Options Indexes Includes FollowSymLinks
AllowOverride None
Order allow, deny
Allow from all
DirectoryIndex index.html index.htm index.shtml index.cgi
Alias /doc/ /usr/doc/
order deny, allow
deny from all
allow from localhost
Options Indexes FollowSymLinks
```

以 RPM 方式安装的 Apache 服务器，配置文件 httpd.conf 存储在 Linux 的＿（5）＿目录下。根据上述配置文件，该 Web 服务器运行在＿（6）＿模式下，其运行效率比在 inetd 模

式下__（7）__；当某个 Web 连接超过__（8）__秒没有数据传输时，系统断开连接。

如果客户需要访问 Linux 服务器上/usr/doc 目录，则应在浏览器地址栏中输入__（9）__。

虚拟主机是指在同一台服务器上实现多个 Web 站点。虚拟主机可以是基于 IP 地址的虚拟主机，也可以是基于__（10）__的虚拟主机。创建基于__（10）__的虚拟主机时，还需要配置__（11）__，并在区数据库文件中添加相关记录。

【问题 3】

下图是配置 Apache 服务器的一个窗口，选中目录选项 ExecCGI，意味着什么？

如果将下图所示的目录选项中 Indexes 选中状态取消，并且虚拟主机目录中也没有相关的 Index 文件，客户机通过浏览器访问有关的虚拟主机目录时有何后果？



试题三分析

本题考查 Web 服务和在 Linux 环境下 Apache 服务器的配置，要求考生能够正确理解 Apache 配置文件。

Web 服务的主要协议是 HTTP（超文本传输协议），HTTP 定义 Web 客户（即浏览器）如何从 Web 服务器请求 Web 页面，以及服务器如何把 Web 页面传送给客户，HTTP 以 TCP（传输控制协议）作为底层协议。当用户请求一个 Web 页面（譬如说点击某个超链接）时，浏览器把请求该页面中各个对象的 HTTP 请求消息发送给服务器。服务器收到请求后，以运送含有这些对象 HTTP 响应消息作为响应。

网络上的资源（包括文字、图片等）可以用 HTML（超文本标记语言）来组织，当 HTML 格式的信息传输到客户机上时，客户有关软件（如 explore 等）根据 HTML 的语法进行解释并显示。

基于 TCP/IP 协议的网络中，应用 URL（统一资源定位符）来标示网络中的资源，URL 的格式为：

```
Scheme://host:port/path?query
```

其中，scheme 为通信协议方案，如 HTTP、FTP、HTTPS 等；host 是资源所在的主机（可以用 IP 地址或有效域名表示）；port 是传输层端口号，如 HTTP 的默认端口是 80；path 是路径，由多个“/”符号隔开的字符串，一般用来表示主机上的一个目录或文件地址；query，查询，可选，用于给动态网页（如使用 CGI、ISAPI、PHP/JSP/ASP/ASP.NET 等技术制作的网页）传递参数，可有多个参数，用“&”符号隔开，参数名和值用“=”符号隔开。支持动态网页的技术有 JSP 和 ASP，其中 JSP 可以跨平台应用。另外，CGI 也是一种动态网页技术，因为存在安全隐患，启动 CGI 需要在配置界面中将 ExecCGI 选中。

所谓虚拟主机服务是指在一台物理机器上提供多个 Web 服务，通常可以采用两种方案：基于 IP 地址的虚拟主机和基于名字的虚拟主机。基于 IP 地址的虚拟主机服务实现需要在机器上配置多个 IP 地址，每个 IP 对应一个虚拟主机。基于名字的虚拟主机可以定义不同的主机名（虚拟的）对应不同的 Web 服务，但是这些虚拟的主机名必须保证能够被正确地进行地址解析，因此需要配置域名解析服务器。

对于 RPM 方式安装的 Apache 服务器，其配置文件存储在“/etc/httpd/conf”目录下，主要配置文件为 httpd.conf，其所有的配置信息均保存在该文件中，更改文件中的配置信息就更改了 Web 服务器的运行模式，图形化配置方式也是以配置该文件为基础的。该文件中的一些主要参数含义如下：

（1）ServerType standalone | inetd　（注：| 表示可选项）

Apache 服务器有两种运行模式：standalone（独立的）和 inetd（作为 inetd 守护进程的子进程运行）。standalone 模式下，不存在对每个请求启动新进程的开销，效率较高，而 inetd 模式的安全性较高。

（2）Timeout 300

该参数指定当某个 Web 访问的 TCP 连接超过多少时间（单位秒）没有数据传输，即认为是连接超时而断开连接。

（3）Port 8080

Apache 服务端口，默认值为 80。

（4）ServerAdmin root@webtest.com.cn

Apache 服务器管理员的电子邮件。服务器可将其运行状态通过这个邮箱发送给管理员。

（5）Alias /doc/ /usr/doc/

定义别名。将真实目录/usr/doc/ 定义为/doc，客户可以通过 http://主机名/doc 访问/usr/doc 目录中的资源。

参考答案

【问题 1】

（1）G. HTTP

（2）F. URL

（3）C. JSP

（4）A. HTML

【问题 2】

（5）/etc/httpd/conf

（6）standalone

（7）高

（8）300

（9）http://服务器 IP 地址（或主机名）:8080/doc/

（10）名称（或名字，域名）

（11）DNS，或域名解析服务

【问题 3】

选中目录选项 ExecCGI，意味着准许执行 CGI

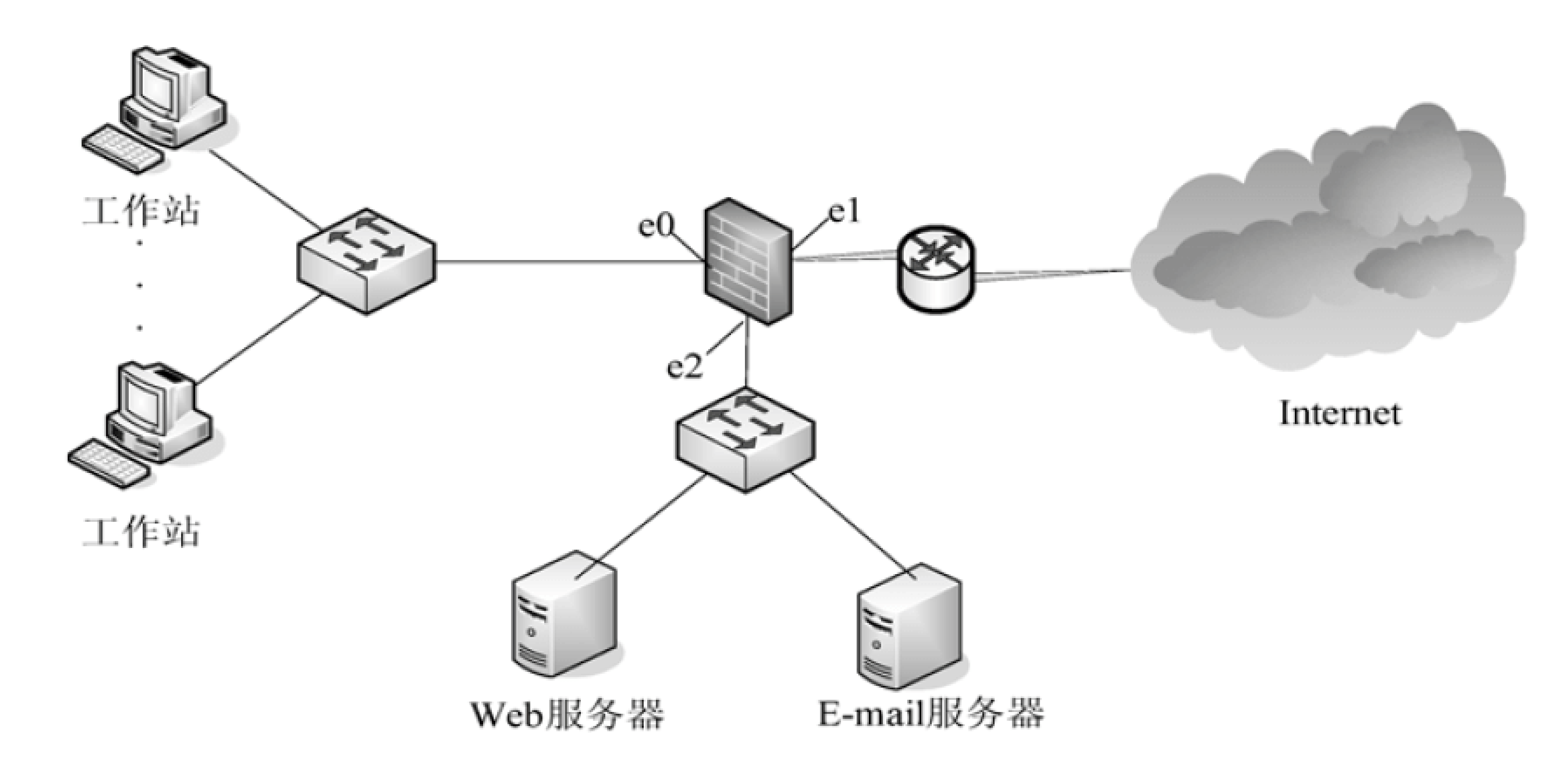
如将 Indexes 选中状态取消，则不允许客户机浏览器在虚拟主机没有 Index 文件时显示目录所有文件。

试题四（15 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某公司采用 100M 宽带接入 Internet，公司内部有 15 台 PC 机，要求都能够上网。另外有 2 台服务器对外分别提供 Web 和 E-mail 服务，采用防火墙接入公网，拓扑结构如下图所示。



【问题 1】

如果防火墙采用 NAPT 技术，则该单位至少需要申请<u>（1）</u>个可用的公网地址。

【问题 2】

下面是防火墙接口的配置命令：

```
fire(config)# ip address outside 202.134.135.98 255.255.255.252
fire(config)# ip address inside 192.168.46.1 255.255.255.0
fire(config)# ip address dmz 10.0.0.1 255.255.255.0
```

根据以上配置，写出上图中防火墙各个端口的 IP 地址：

e0：____（2）____

e1：____（3）____

e2：____（4）____

【问题 3】

1．ACL 默认执行顺序是__（5）__，在配置时要遵循__（6）__原则、最靠近受控对象原则、以及默认丢弃原则。

（5）、（6）备选项

（A）最大特权　　（B）最小特权　　（C）随机选取

（D）自左到右　　（E）自上而下　　（F）自下而上

2．要禁止内网中 IP 地址为 192.168.46.8 的 PC 机访问外网，正确的 ACL 规则是（7）

（A）access-list 1 permit ip 192.168.46.0 0.0.0.255 any
　　access-list 1 deny ip host 192.168.46.8 any

（B）access-list 1 permit ip host 192.168.46.8 any
　　access-list 1 deny ip 192.168.46.0 0.0.0.255 any

（C）access-list 1 deny ip 192.168.46.0 0.0.0.255 any
　　access-list 1 permit ip host 192.168.46.8 any

（D）access-list 1 deny ip host 192.168.46.8 any
　　access-list 1 permit ip 192.168.46.0 0.0.0.255 any

【问题 4】

下面是在防火墙中的部分配置命令，请解释其含义：

global (outside) 1 202.134.135.98-202.134.135.100　　____（8）____

conduit permit tcp host 202.134.135.99 eq www any　　____（9）____

access-list 10 permit ip any any　　____（10）____

试题四分析

本题考查的是防火墙的配置。

【问题 1】

本题考查的是 NAT 技术的使用。

在使用防火墙时，NAT 技术主要用于连接和安全方面。目前企业内部网络用户数量

大，而能申请的合法的全球唯一 IP 地址有限。NAT 能够有效的解决企业 IP 地址短缺问题，利用 NAT 技术能够实现多个用户共同使用一个合法的 IP 地址连接互联网。NAT 包括有静态 NAT、动态地址 NAT 和端口多路复用地址转换 3 种技术类型。静态 NAT 是把内部网络中的每个主机地址永久映射成外部网络中的某个合法地址；动态地址 NAT 是采用把外部网络中的一系列合法地址使用动态分配的方法映射到内部网络；端口多路复用地址转换是把内部地址映射到外部网络的一个 IP 地址的不同端口上。根据不同的需要，选择相应的 NAT 技术类型。

如果 ISP 提供的合法 IP 地址数量较多，当然可以采用静态地址转换+端口复用动态地址转换技术实现。如果只获得 1 个合法 IP 地址，可以采用 TCP/UDP 端口 NAT 映射。既然只有一个可用的合法 IP 地址，当然采用端口复用方式来实现 NAT。不过，由于同时有要求网络内部的服务器要被 Internet 访问到，因此必须采用 PAT 创建 TCP/UDP 端口的 NAT 映射。

所以根据题目要求，该单位至少应有 1 个公网 IP 地址。

【问题 2】

本题考查的是防火墙结构。

根据配置可知，该防火墙外网 IP 地址为 202.134.135.98，内网 IP 地址为 192.168.46.1，DMZ 区的 IP 地址为 10.0.0.1。

从本题的示意图可知，防火墙 e0 口连接内部工作站，为内网接口；防火墙 e1 口连接 Internet，为外网接口；防火墙 e2 口连接内部服务器，为 DMZ 接口。所以：

e0：192.168.46.1

e1：202.134.135.98

e2：10.0.0.1

【问题 3】

本题考查的是 ACL 执行原则。

1．ACL 默认的执行次序是自上而下，另外 ACL 在执行时应注意以下原则：

（1）最小特权原则

只给受控对象完成任务所必须的最小的权限。也就是说被控制的总规则是各个规则的交集，只满足部分条件的是不容许通过规则的。

（2）最靠近受控对象原则

所有的网层访问权限控制。也就是说在检查规则时是采用自上而下在 ACL 中一条条检测的，只要发现符合条件了就立刻转发，而不继续检测下面的 ACL 语句。

（3）默认丢弃原则

在CISCO路由交换设备中默认最后一句为 ACL 中加入了 DENY ANY　ANY，也就

是丢弃所有不符合条件的数据包。这一点要特别注意，虽然我们可以修改这个默认，但未改前一定要引起重视

2．ACL 在执行时，默认的执行次序是自上而下。另外，在匹配规则时，数据包如果与前面的规则已匹配，就会按照此规则执行，而不再匹配下面与该数据包相关的规则。

要禁止内网中 IP 地址为 192.168.46.8 的 PC 机访问外网。需要先禁止 192.168.46.8 数据包，再放行 192.168.46.0 网段数据包，注意次序。

【问题 4】

本题考查的 ACL 规则。各规则解释如下：

```
global (outside) 1 202.134.135.98-202.134.135.100
//指定外网口 IP 地址范围为 202.134.135.98-202.134.135.100
conduit permit tcp host 202.134.135.99 eq www any
//允许任意外网主机访问 202.134.135.99 提供的 WWW 服务
access-list 10 permit ip any any
//允许任意 IP 数据包进出
```

参考答案

【问题 1】

（1）1

【问题 2】

（2）192.168.46.1

（3）202.134.135.98

（4）10.0.0.1

【问题 3】

（5）（E）自上而下

（6）（B）最小特权

（7）（D）access-list 1 deny ip host 198.168.46.8 any

access-list 1 permit ip 192.168.46.0 0.0.0.255 any

【问题 4】

（8）指定外网口 IP 地址范围为 202.134.135.98-202.134.135.100

（9）允许任意外网主机访问 202.134.135.99 提供的 WWW 服务

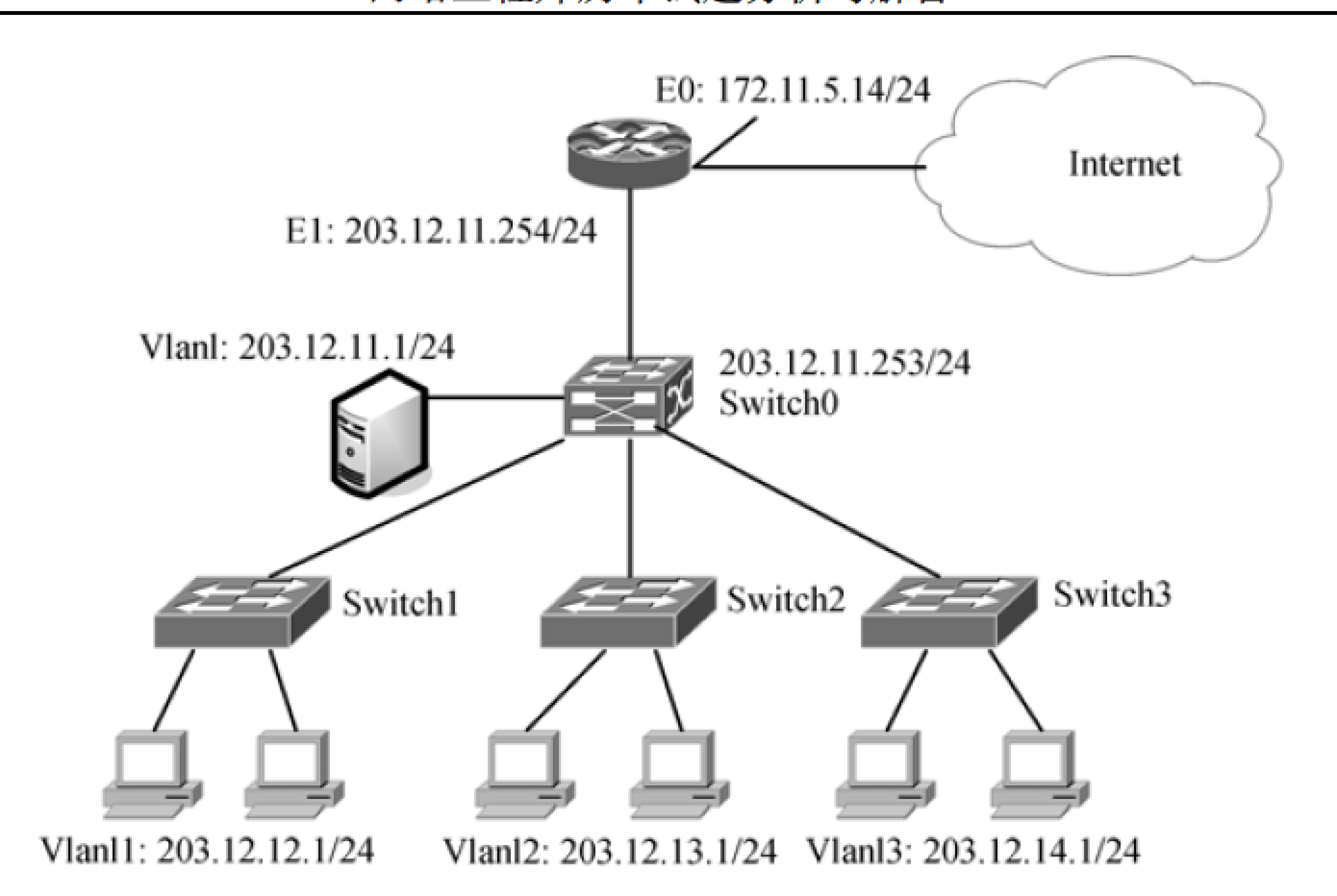
（10）允许任意 IP 数据包进出

试题五（15 分）

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

某公司租用了一段 C 类地址 203.12.11.0/24～203.12.14.0/24，如下图所示。其网间地址是 172.11.5.14/24。要求网内所有 PC 都能上网。



【问题 1】

接入层交换机 Switch1 的端口 24 为 trunk 口，其余各口属于 vlan11，请解释下列命令并完成交换机的配置。

Switch1#config terminal
Switch1(config)#interface f0/24 （进入端口 24 配置模式）
Switch1(config-if)# switchport mode trunk ____（1）____
Switch1 (config-if)#switchport trunk encapsulation dotlq ____（2）____
Switch1(config-if)# switchport trunk allowed all（允许所有 VLAN 从该端口交换数据）
Switch1(config-if)#exit
Switch1(config)#exit
Switch1# vlan database
Switch1(vlan)# vlan 11 name lab01 ____（3）____
Switch1(vlan)#exit
Switch1#config terminal
Switch1(config)#interface f0/9 （进入 f0/9 的配置模式）
Switch1(config-if)#____（4）____ （设置端口为接入链路模式）
Switch1(config-if)#____（5）____ （把 f0/9 分配给 VLAN11）
Switch1(config-if)#exit
Switch1(config)#exit

【问题 2】

以下两个配置中错误的是____（6）____，原因是____（7）____。

A．Switch0 (config)#interface gigabitEthernet 0/3
Switch0 (config-if)#switchport mode trunk
Switch0 (config-if)#switchport trunk encapsulation dot1q
Switch0(config)#exit

Switch0# vlan database
Switch0(vlan)# vlan 2100 name lab02

B．Switch0 (config)#interface gigabitEthernet 0/3
Switch0 (config-if)#switchport mode trunk
Switch0 (config-if)#switchport trunk encapsulation ISL
Switch0(config)#exit
Switch0# vlan database
Switch0(vlan)# vlan 2100 name lab02

【问题 3】

Switch1 的 f0/24 口接在 Switch0 的 f0/2 口上，请根据本题的示意图完成或解释以下 Switch0 的配置命令。

Switch0(config)# interface__（8）__　　（进入虚子接口）
Switch0(config-if)# ip address 203.12.12.1 255.255.255.0（加 IP 地址）
Switch0(config-if)# no shutdown　　__（9）__
Switch0(config-if)# standby 1 ip 203.12.12.253　　（建 HSRP 组并设虚 IP 地址）
Switch0(config-if)# standby 1 priority 110　　__（10）__
Switch0(config-if)# standby 1 preempt　　__（11）__

试题五分析

本题考查的是交换机 vlan 的配置。

【问题 1】

由题目要求可知，Switch1 的端口 24 为 trunk 口，其余各口属于 vlan11，故 Switch1 的配置及解释如下。

```
Switch1#config terminal
Switch1(config)#interface f0/24                （进入端口 24 配置模式）
Switch1(config-if)# switchport mode trunk     设置端口为中继模式
Switch1 (config-if)#switchport trunk encapsulation dotlq 设置 Trunk 采用
802.1q 格式
Switch1(config-if)# switchport trunk allowed all（允许所有 VLAN 从该端口交
换数据）
Switch1(config-if)#exit
Switch1(config)#exit
Switch1# vlan database
Switch1(vlan)# vlan 11 name lab01             创建 vlan11，并命名为 lab01
Switch1(vlan)#exit
Switch1#config terminal
Switch1(config)#interface f0/9                 （进入 f0/9 的配置模式）
Switch1(config-if)# switchport mode access    （设置端口为接入链路模式）
Switch1(config-if)# switchport access vlan11  （把 f0/9 分配给 VLAN11）
Switch1(config-if)#exit
Switch1(config)#exit
```

【问题 2】

本题考查的是 VLAN 数据帧的封装模式。

在实现 VLAN 时，为了标识各数据帧属于哪一个 VLAN，需要对流经汇聚链接的数据帧进行封装，以附加上 VLAN 信息，这样交换机就可通过 VLAN 标识，将数据帧转发到对应的 VLAN 中。

目前交换机支持的封装协议有 IEEE802.1Q 和 ISL。其中 IEEE802.1Q 是经过 IEEE 认证的对数据帧附加 VLAN 识别信息的协议，属于国际标准协议，适用于各个厂商生产的交换机，该协议通常也简称为 dot1q。ISL 是 Inter Switch Link 的缩写，是 Cisco 系列交换机支持的一种用于在汇聚链路上附加 VLAN 信息的协议。

以上两种封装协议在使用范围、数据帧格式上是不同的。另外，ISL 最多支持 1024 个 VLAN，802.1Q 加上扩展 VLAN 可支持 4096 个，有 2 个是被保留，所以可用 4094 个。

从以上分析可知，只有 dot1q 封装协议支持超过 1024 个 vlan ，而题目中配置的 vlan ID 为 2100，已超过 1024，故 B 选项是错误的。

【问题 3】

本题考查的是核心层交换机的 vlan 配置。Switch0 交换机的配置及解释如下：

```
Switch0(config)# interface___(8)___                 （进入虚子接口）
Switch0(config-if)# ip address 203.12.12.1 255.255.255.0    （加 IP 地址）
Switch0(config-if)# no shutdown 开启端口
Switch0(config-if)# standby 1 ip 203.12.12.253 （建 HSRP 组并设虚 IP 地址）
Switch0(config-if)# standby 1 priority 110      设优先级
Switch0(config-if)# standby 1 preempt           设切换许可
```

参考答案

【问题 1】

（1）设置端口为中继（或 Trunk）模式

（2）设置 Trunk 采用 802.1q 格式（或 dot1q）

（3）创建 vlan11，并命名为 lab01

（4）switchport mode access

（5）switchport access vlan11

【问题 2】

（6）B

（7）trunk 采用 ISL 格式时，vlan ID 最大为 1023

【问题 3】

（8）vlan11

（9）开启端口

（10）设优先级

（11）设切换许可